National Défense
Defence nationale

B-GL-300-005/FP-001

LAND FORCE
INFORMATION OPERATIONS
(ENGLISH)

WARNING

ALTHOUGH NOT CLASSIFIED, THIS PUBLICATION, OR ANY PART OF IT, MAY BE EXEMPTED FROM DISCLOSURE TO THE PUBLIC UNDER THE ACCESS TO INFORMATION ACT. ALL ELEMENTS OF INFORMATION CONTAINED HEREIN MUST BE CLOSELY SCRUTINIZED TO ASCERTAIN WHETHER OR NOT THE PUBLICATION, OR ANY PART OF IT, MAY BE RELEASED.

(This publication is effective on receipt.)

Issued on Authority of the Chief of the Defence Staff

OPI: DAD 5

1999-01-18

Canada

FOREWORD

1. B-GL-300-005/FP-001, *Information Operations*, is issued on the authority of the Chief of the Defence Staff.

2. This publication is effective on receipt.

3. Suggestions for amendments should be forward through normal channels to the Director Army Doctrine, Attention DAD 5, Fort Frontenac, PO Box 17000 Station Forces, Kingston, ON, K7K 7B4.

4. Unless otherwise noted, masculine pronouns apply to both men and women.

5. The NDID for the French version of this publication is B-GL-300-005/FP-002. The terminology used in this publication is consistent with the Army vocabulary.

PREFACE

GENERAL

1. This doctrine manual describes a multidimensional concept used by the Army to achieve success across the continuum of operations. The Army has embraced Information Operations (IO) as an essential combat function that must be integrated with the remainder of the combat functions to maximize combat power. The elements of IO are not new; some have been present in warfare for thousands of years. What is new is the emphasis on the integration of these elements to maximize combat power. The aim of IO is information superiority gained by the optimum exploitation of information and by denying the same capability to any adversary.

PURPOSE

2. The purpose of B-GL-300-005/FP-001, *Information Operations,* is to describe the concept in detail, and outline how IO relates to other combat functions and contributes to the success of commanders on the battlefield.

SCOPE

3. The heart of this concept is the notion of two information environments, namely the Global Information Environment (GIE) and the Military Information Environment (MIE). These environments bring together in a civil and military context all agencies, groups, individuals, systems, and procedures that deal with information. This operational activity is dynamic, complex and requires a great deal of co-ordination. It brings many traditionally separate disciplines and new technologies together to provide the commander with the information superiority needed for success.

4. The Army has packaged this combat function into six components broken into:

a. four support components:

(1) Communication Information Systems (CIS),

(2) Relevant Information, including intelligence, surveillance, target acquisition and reconnaissance (ISTAR),

(3) Civil-military Cooperation (CIMIC), and

(4) Public Affairs (PA); and

b. two action components:

(1) Offensive Information Operations (Off IO), and

(2) Defensive Information Operations (Def IO).

5. IO, as a combat function encompasses a human, a moral, a physical and an electromagnetic dimension. The doctrine and concepts outlined in this publication are applicable to the operational and tactical levels of command across the full spectrum of conflict. Strategic level IO doctrine is contained in B-GG-005-004/AF-032, *Canadian Forces Information Operations*.

TABLE OF CONTENTS

FOREWORD i

PREFACE iii

General iii

Purpose iii

Scope iii

CHAPTER 1 INFORMATION OPERATIONS AND THE OPERATING ENVIRONMENT

SECTION 1 INTRODUCTION 1

SECTION 2 INFORMATION OPERATIONS CONCEPT 2

SECTION 3 THE OPERATING ENVIRONMENT 5

SECTION 4 TECHNOLOGY 7

SECTION 5 INFORMATION MANAGEMENT 13

CHAPTER 2 FUNDAMENTALS, COMPONENTS AND ACTIVITIES

SECTION 1 INTRODUCTION 15

SECTION 2 FUNDAMENTALS 15

SECTION 3 COMPONENTS 16

Communication Information Systems 17

Architecture 18

Integration 19

Global Connectivity 19

Information Management 20

Relevant Information 20

Public Affairs 23

Civil-Military Cooperation 24

Offensive and Defensive Information Operations 25

Offensive Information Operations 25

Defensive Information Operations 25

SECTION 4 ACTIVITIES 26

Acquire 27

Use 27

Exploit 28

Verify 29

Manage 30

Protect 31

Deny 32

SECTION 5 INTEGRATION WITH OTHER COMBAT FUNCTIONS 33

Command 33

Protection 33

Firepower 34

Manoeuvre 34

Sustainment 34

CHAPTER 3 COMMUNICATION AND INFORMATION SYSTEMS

SECTION 1 THE ENVIRONMENT 37

SECTION 2 FUNCTIONS 38

SECTION 3 ROLE 40

SECTION 4 MILITARY INFORMATION SYSTEMS 41

SECTION 5 NON-MILITARY INFORMATION SYSTEMS 43

SECTION 6 PLANNING OF COMMUNICATION AND INFORMATION SYSTEMS 44

Non-military Information Systems 44

Training 44

Communications Support 45

Capabilities 46
Future Technology 46
Security 47
Communication and Information Systems Management 48

CHAPTER 4 RELEVANT INFORMATION

SECTION 1 INTRODUCTION 51
SECTION 2 RELEVANT INFORMATION 51
SECTION 3 ASSESSMENT CRITERIA 52
SECTION 4 INTELLIGENCE 55
Role of Intelligence 55
Intelligence-Enabling Functions 56
Assessing Friendly Vulnerabilities—
Counter-Intelligence 56
Understanding the Adversary 57
SECTION 5 EMPLOYING INTELLIGENCE—
PREPARATION OF THE BATTLEFIELD 57
SECTION 6 ASSESSING BATTLE DAMAGE 59

CHAPTER 5 INTELLIGENCE, SURVEILLANCE, TARGET ACQUISITION AND RECONNAISSANCE IN LAND OPERATIONS

SECTION 1 INTRODUCTION 61
SECTION 2 THE ISTAR CONCEPT 62
SECTION 3 THE PRINCIPLES OF ISTAR 63
SECTION 4 THE ACTIVITIES OF ISTAR 64
SECTION 5 SOURCES AND AGENCIES 66
SECTION 6 ISTAR PLANNING AND EXECUTION 68
SECTION 7 THE TARGETING PROCESS 69

CHAPTER 6 OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS

SECTION 1 INTRODUCTION 71

Role of Offensive and Defensive Information Operations 72

SECTION 2 ELEMENTS 73

Relevant Information 73

Communication Information Systems 74

Operations Security 74

Counter-Intelligence 75

Military Deception 75

Psychological Operations 76

Counter-Psyops 77

Electronic Warfare 77

Computer Network Attack 79

Special Information Operations 79

Physical Destruction 79

SECTION 3 OFFENSIVE INFORMATION OPERATIONS 80

SECTION 4 DEFENSIVE INFORMATION OPERATIONS 82

SECTION 5 CO-ORDINATION 85

CHAPTER 7 PUBLIC AFFAIRS

SECTION 1 INTRODUCTION 87

SECTION 2 INFORMATION ENVIRONMENT 88

SECTION 3 ROLE OF PUBLIC AFFAIRS IN SUPPORT OF INFORMATION OPERATIONS 89

SECTION 4 PUBLIC AFFAIRS PLANNING CONSIDERATIONS 93

SECTION 5 COMMAND AND CONTROL OF PUBLIC AFFAIRS 95

CHAPTER 8 CIVIL-MILITARY COOPERATION

SECTION 1 INTRODUCTION AND DEFINITIONS 97

SECTION 2 ARMY OBJECTIVES IN CIVIL-MILITARY COOPERATION 99

SECTION 3 TYPES OF CIVIL-MILITARY COOPERATION 101

SECTION 4 CIVIL-MILITARY COOPERATION, PSYCHOLOGICAL OPERATIONS AND PUBLIC AFFAIRS RELATIONSHIPS 102

SECTION 5 INFORMATION SOURCES 103

SECTION 6 CIMIC AND INFORMATION PROCESSING 105

SECTION 7 LIMITATIONS/UNAUTHORIZED ACTIVITIES 106

ANNEX A MUTUAL SUPPORT WITHIN THE ELEMENTS OF OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS 123

TABLE OF FIGURES

Figure 1-2-1: Commander's Decision-Action Cycle 3
Figure 1-3-2: The Multi-Dimensional Area of Operations 6
Figure 1-4-3: The Advantages of Data and Information Fusion 9
Figure 1-4-4: Key Technology Areas for Battlefield Visualization 10
Figure 1-4-5: The Cognitive Hierarchy and the Art of Operations 11
Figure 2-3-1: Global Information Environment 17
Figure 2-4-2: Information Operations Activities 26
Figure 3-1-1: Increasing Speed in Flow & Processing of Information Throughout the Ages 38
Figure 3-3-2: Global Communications Network 41
Figure 3-4-3: Land Force Communication Information Systems 43
Figure 4-2-1: Relevant Information 52
Figure 8-1-1: CIMIC and the Spectrum of Conflicts 98
Figure 8-2-2: The Operational Environment 101
Figure 8-3-3: Types of Civil-Military Cooperation 102

CHAPTER 1
INFORMATION OPERATIONS AND THE OPERATING ENVIRONMENT

Victory smiles upon those who anticipate changes in the character of war, not upon those who wait to adapt themselves after the changes occur[1]

General Gulio Douhet (1869-1930)

SECTION 1
INTRODUCTION

1. The aim of this chapter is to introduce the concept of Information Operations (IO) and describe the environment, and technology that are relevant to IO. There are a number of trends, which are having a significant effect on the battlefield including the asymmetric application of combat power, the growing non-linearity and non-contiguous nature of the battlefield, and the increased importance of *"information age warfare"*[2] concepts and technologies. Many books and articles have been written on these subjects. The one thing they have in common is the description of increased dependence on information of modern armies and the great increase in information that is available today. This does not only include the amount of information that is of concern but also the nature, availability, speed, complexity and the growing dependence on this information and the technology that acquires, processes, distributes and stores this information.

2. IO are an essential element of combat power that allows modern commanders to exercise Mission Command within the manoeuvrist approach to operations in the information age.IO are not new. In their

---

[1] General Giulio Douhet is often referred, in the military historian community, as the Clausewitz of air strategy. An Italian artillery officer, before the First World War, he secured command of the Italian Army's first air unit and practised aerial bombardment in Libya during the Italo-Turkish war of 1911-12. His ambitious air strategy ideas, set out in his book *Command of the Air (Il Dominio dell' aria)* recognised, as early as 1915, that the aircraft was a weapon of limitless offensive power.

[2] Alvin & Hiedi Toffler, *War and Anti War: The Third Wave*, (New York: Morrow, 1980).

simplest form they encompass all operations that gain information and knowledge that enhances friendly execution of operations, while denying the enemy similar capabilities by whatever means possible.

3. IO are not new. In their simplest form they encompass all operations that gain information and knowledge that enhances friendly execution of operations, while denying the enemy similar capabilities by whatever means possible.

4. Proper integration of IO will help our forces seize the initiative and remain physically and mentally more agile than the enemy at the right time and place, with the right weapons and resources.

SECTION 2
INFORMATION OPERATIONS CONCEPT

5. The principal objective of IO is to achieve superiority and relative advantage between the friendly commander's decision-action cycle (see Figure 1-2-1) and that of the adversary, and to use that advantage to enhance and enable other elements of combat power. As shown in Figure 1-2-1 the application of IO can enhance battlefield visualization, improve designation of main effort, improve control of operational tempo, and improve synchronisation.

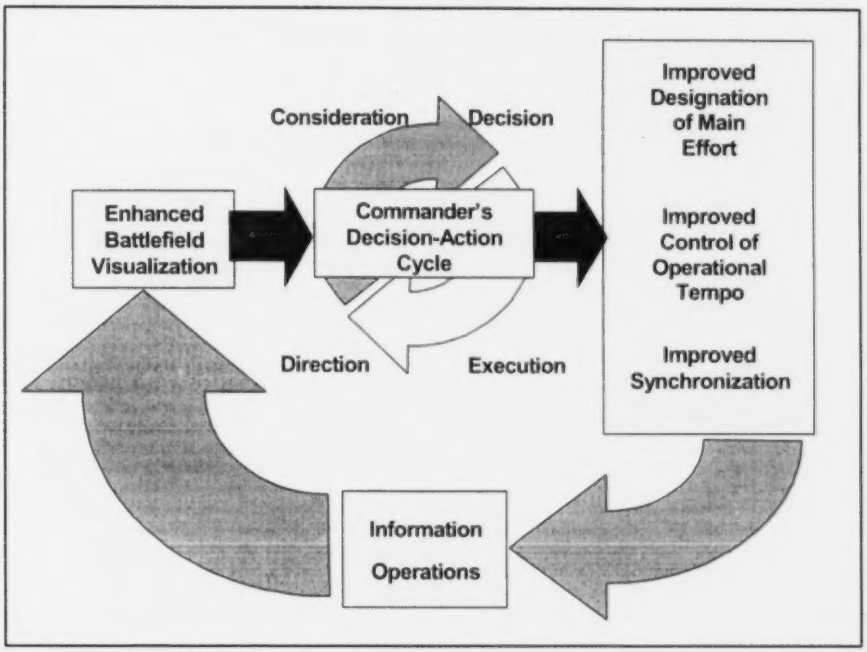

Figure 1-2-1: Commander's Decision-Action Cycle

6. The ideal state of operations is one in which we achieve information dominance. Absolute and sustained dominance of the expansive information environment is not possible. Commanders seek to achieve information superiority at the right place, the right time, and in the right circumstances. Information superiority, is the disparity between what friendly forces know about their Area of Operations (AO) and operations within it and what the enemy knows.

7. The combative nature of IO means that information superiority is neither continuous nor assured. Army commanders seek sustained information superiority in their areas of operation. In some cases, especially early in an operation, they may have to settle for local or temporary superiority generated at critical junctures of their operation. Even when possessing general information superiority, enemy forces may have niche capabilities that overmatch some aspects of friendly forces' capabilities. Operational Commanders work to minimize situations in which friendly forces engage under tactical conditions of information parity or inferiority. This is not a panacea though, Commanders will still need to take risks and will not have the luxury of waiting for the perfect knowledge and plan.

8. The heart of this concept is the notion of an information universe that encompasses all aspects of our society and pervades all levels of military action from the grand strategic level to the lowest tactical level. In an attempt to create some order to this universe, it has been subdivided into two distinct environments, the Global Information Environment (GIE) and the Military Information Environment (MIE) (see Figure. 2-3-1, Chapter 2). These groupings bring together in a civil and military context all agencies, groups, individuals, systems and procedures that deal with information. This manual will concentrate on the MIE. In this context IO bring together many traditionally separate disciplines and new technologies to provide the commander with information superiority and the capability to achieve success.

9. IO are designed to enhance or magnify the effect of friendly combat power and diminish that of the enemy. A key IO function is to paralyze, disorganize, or degrade the enemy's ability to apply his IO systems. IO may be offensive or defensive. The Army Doctrine packages this concept into six components broken into:

a. four support components:

(1) Communication Information Systems (CIS),

(2) Relevant Information, including Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR),

(3) Civil-military Cooperation (CIMIC), and

(4) Public Affairs (PA); and

b. two action components:

(1) Offensive Information Operations (Off IO), and

(2) Defensive Information Operations (Def IO).

10. Most often IO objectives will be vertically integrated to support and gain leverage from higher headquarters IO capabilities. These objectives may be established as high as government and integrated

vertically through subordinate commanders. IO must also be integrated horizontally. IO must be synchronized with the other combat functions to maximize combat power. Planning and execution of IO are not done in isolation and are therefore integrated in B-GL-331-001/FP-001, *Command Support Doctrine*.

11. IO also include exploitation of the Army's own tactical assets to enhance its knowledge. It entails not only collecting information, which still needs to be analysed to be useful, but also sharing it with higher, lower, and adjacent units so that all are operating from a common relevant picture. This sharing of information will also include; joint, combined, Governmental Organisations, Non-Governmental Organizations (NGOs), and Supra National Organisations such as the United Nations (UN) or the Organization of American States (OAS).

SECTION 3
THE OPERATING ENVIRONMENT

12. IO allow us to operate in expanded areas of operation. The AO now goes beyond the traditional physical dimensions of time, width, depth, and height. It also includes the Electro-Magnetic spectrum (Figure 1-3-2). The AO also extends beyond the physical boundaries of tactically deployed formations through their communications and connectivity to other land, joint and coalition elements, even reaching back to Canada from the theatre of operations. The AO will also be defined by the human dimensions: which includes not only soldiers, and leaders, but also the civilian population in the theatre of operations and the citizens of Canada and the rest of the world. AOs, in particular those at the operational level, will be framed not only by the application of traditional elements of physical combat power, but also by Deception, Psychological Operations (PSYOPS), CIMIC, and PA.

13. The potential influence of IO further depends on the command architecture. If an adversary presents a rigid hierarchical command structure, then cutting the links "between the head and the body" will immobilise the body. Other conflict situations may provide adversaries that allow field commanders more autonomy. In this case, an attack on central authority could conceivably allow field commanders to exercise an initiative that would more than compensate for the destruction of the central co-ordination authority. For example, at the strategic level, operations against an adversary who is believed to have, or does have, weapons of mass destruction, which would lead to the destruction of a

central command centre that exercises positive control over these weapons of mass destruction could be catastrophic.

14. Global communications and information technology have accelerated and expanded collective awareness of events, issues, and concerns. In the moral domain, they ignite passions; spark new perspectives; crystallise deeply held beliefs; and compel people, nations, organisations, and institutions everywhere to examine, define, and act on their interests. While many effects of this phenomenon may be benign and beneficial, others create turbulence, confusion, chaos and conflict. The information universe illustrated earlier in this chapter portrays the extent of this environment.

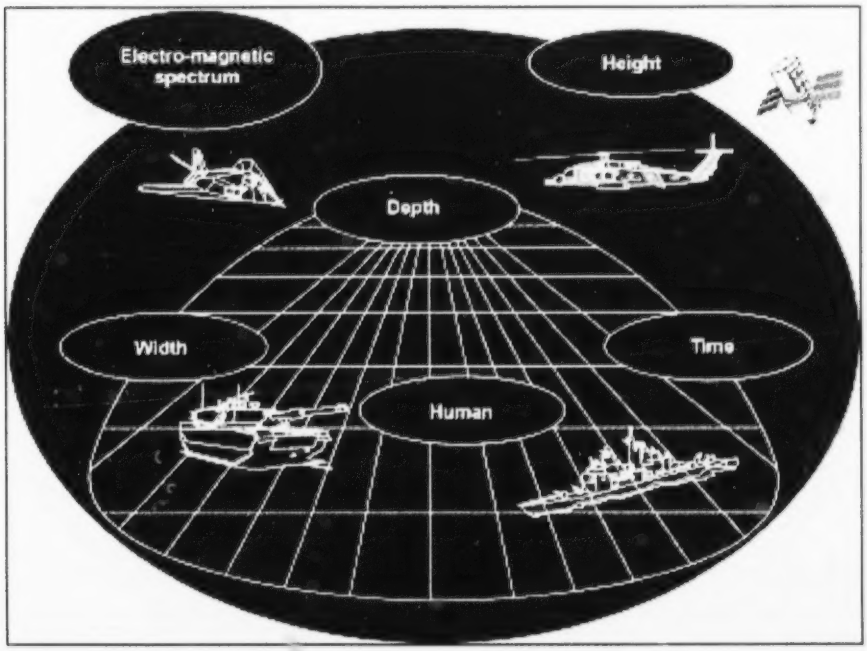

Figure 1-3-2: The Multi-Dimensional Area of Operations

15. IO, therefore, involve more than a force attacking an adversary's information flow while protecting its own. They require awareness of and sensitivity to non-military information sources. These non-military information sources could comprise neutral and or friendly governmental and non-governmental organisations to include paramilitary forces, the media and politically oriented organisations, which can all influence military operations, leadership perceptions and the flow of information through information systems. Some of these information sources are able to provide tactical-level information almost immediately to audiences

central command centre that exercises positive control over these weapons of mass destruction could be catastrophic.

14. Global communications and information technology have accelerated and expanded collective awareness of events, issues, and concerns. In the moral domain, they ignite passions; spark new perspectives; crystallise deeply held beliefs; and compel people, nations, organisations, and institutions everywhere to examine, define, and act on their interests. While many effects of this phenomenon may be benign and beneficial, others create turbulence, confusion, chaos and conflict. The information universe illustrated earlier in this chapter portrays the extent of this environment.

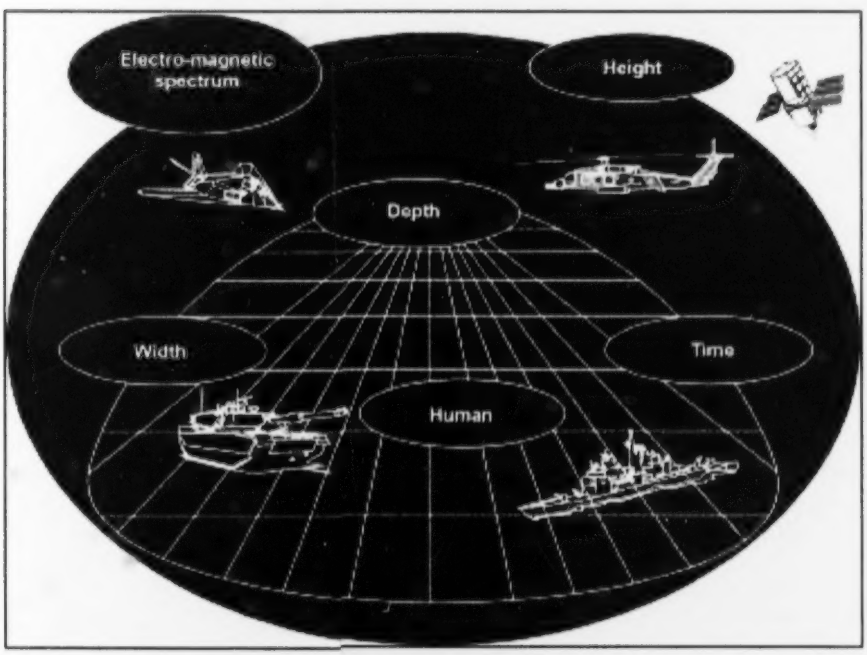

Figure 1-3-2: The Multi-Dimensional Area of Operations

15. IO, therefore, involve more than a force attacking an adversary's information flow while protecting its own. They require awareness of and sensitivity to non-military information sources. These non-military information sources could comprise neutral and or friendly governmental and non-governmental organisations to include paramilitary forces, the media and politically oriented organisations, which can all influence military operations, leadership perceptions and the flow of information through information systems. Some of these information sources are able to provide tactical-level information almost immediately to audiences

throughout the world. Conversely, faraway events can immediately influence operations.

16. The GIE includes all individuals, organisations, or systems, most of which are outside the control of the military or government. The MIE is that portion of the GIE relevant to military operations. The interaction of the GIE and the MIE introduces many more players into the AO, compresses the traditional levels of conflict in time but expand them in space, and gives operations a simultaneous and continuous character. Tactical military operations are more likely to have political and social implications, requiring additional focus on non-military factors in planning and execution. Commanders must understand the comprehensive civil and military end state and not just the military conditions of that end state.

SECTION 4
TECHNOLOGY

17. As stated earlier new technologies have revolutionised the information universe and the MIE. Areas of operation and interest have increased at all levels of command primarily due to reduced force levels, better mobility, better weapon system capabilities of both friendly and enemy forces, as well as increased situational awareness (SA) and the ability to network sensors and their data. Digital data communication is greatly increasing the volume and speed with which information is passed between points/elements on the battlefield. Some form of aggregation and fusion of data and information will have to occur in order to avoid becoming overwhelmed with new, recurring, redundant, and irrelevant information.

18. SA will only be achieved if the information provided is coherent, relevant and timely. Information, which is not time sensitive or of a repeating nature can be aggregated by subject, entity, or time and stored until required. Information of tactical importance needs to be passed by the fastest means possible and presented in a standardised format, which can be understood by all. Initially, incoming information should be screened for its timeliness, format, correctness, and stored in a message database. The information needs to be compared to other pieces of similar information and investigated if it does not agree with the information already available. This additional information will expand the information equation and may require additional expertise for the analysis

process. The advantages of this data and information fusion are portrayed in Figure 1-4-3.

19. Technology has also affected another aspect of the battlefield and that is the ability to visualise the battlefield. Battlefield Visualization (BV) is defined as *"the process whereby the commander develops a clear understanding of his current state with relation to the adversary and the environment, envisions a desired end state, and then subsequently visualises the sequence of activity to this end state."* BV has two components: the art of BV, which is a human process that can be developed in all of us to a greater or lesser degree, and the science of BV, which deals with the technology that can enhance our human capabilities.

20. BV is an important element of our ability to gain information superiority at critical times and places on the battlefield. This superiority will enable a smaller force to rapidly overwhelm a larger foe, and allow tactical formations to enforce extended zones of separation or conduct humanitarian relief operations across a distributed battlefield. The science of BV has three primary components:

a. Situational Awareness, which answers the questions:

(1) Where am I?

(2) Where are my friends?

(3) Where is the enemy?

b. Environment Visualization, which provides information on all aspects of the environment where operations are conducted and includes, as an example: space, geospatial information, geography, meteorology, electromagnetic spectrum, sociology and legal.

c. Asset Visibility, which provides the commander with an accurate status of human, materiel and information resources.

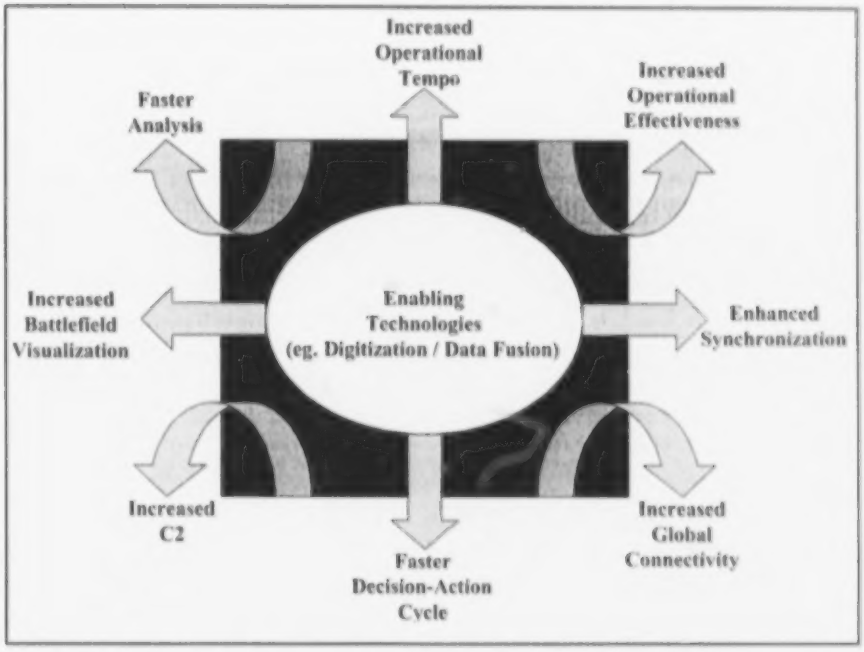

Figure 1-4-3: The Advantages of Data and Information Fusion

21. Information technology advances have provided many tools including displays, storage, databases, archival search and retrieval, target recognition, sensors and networks (see Figure 1-4-4). Human skills must proceed apace in order to integrate the application of technological advances to the process of IO. Similarly, those selected for command must understand IO processes and be familiar with the underlying human skills and technologies if they are to fully appreciate, access and shape BV.

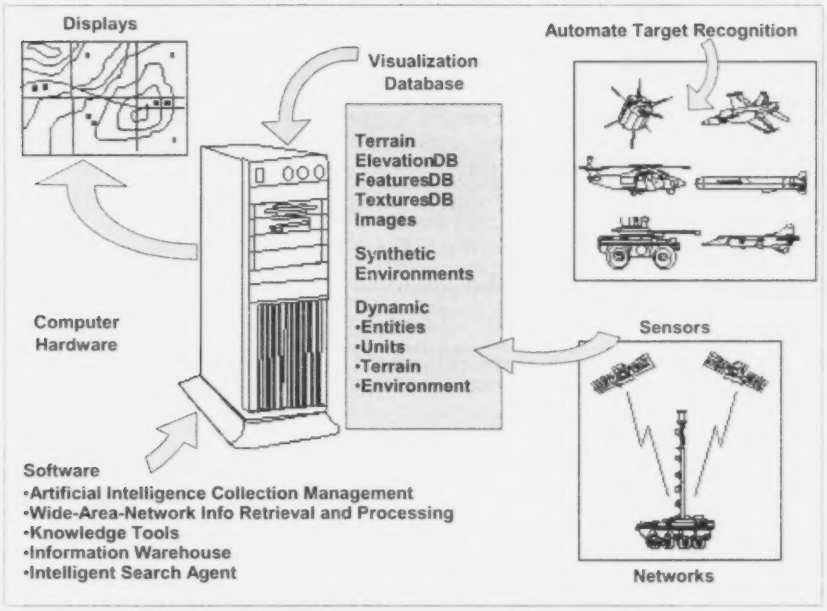

Figure 1-4-4: Key Technology Areas for Battlefield Visualization

22. Another key growth area in information technology provides the tools to assist the transition from data to understanding. Military operations must account for an environment of certainty, risk and friction – the eternal Clausewitzian concept of the "Fog of War." Information may be incomplete, unreliable, ambiguous, or even contradictory. There are four levels of uncertainty:

a. Data-uncertainty regarding what is being observed: Is this report accurate? Are the forces observing the key activities?

b. Information-uncertainty as to the facts: Where is the enemy and in what numbers?

c. Knowledge-uncertainty regarding what to infer from known facts: What are the enemy's intentions? What is his state of morale?

d. Understanding- uncertainty regarding the outcome of actions: Can the forces turn the enemy's flank? Will success at this point cause his collapse?

23. Many military activities are uncertain because they defy prediction. There is much that both friendly forces and the adversary cannot foresee or control. Information technology will never eliminate the effects of uncertainties nor will it ever eliminate them all. Instead, Information Technology will provide commanders and staff with tools to "manage" uncertainties within an accepted level of risk. In the absence of knowledge and understanding, more data can even increase uncertainty.

24. A significant challenge in the GIE and the MIE is the selection and sorting of the huge volume of data available to the commander. Data must not be confused with understanding (see Figure 1-4-5). Sensor observations relevant to the AO are mere data until they are processed into an organised, useful format as information. Although, SA is inherently local and relevant to a particular echelon of the military force, digitization facilitates the sharing of SA both vertically and horizontally. Shared, SA reinforces overall SA and enables decentralised execution throughout the command.

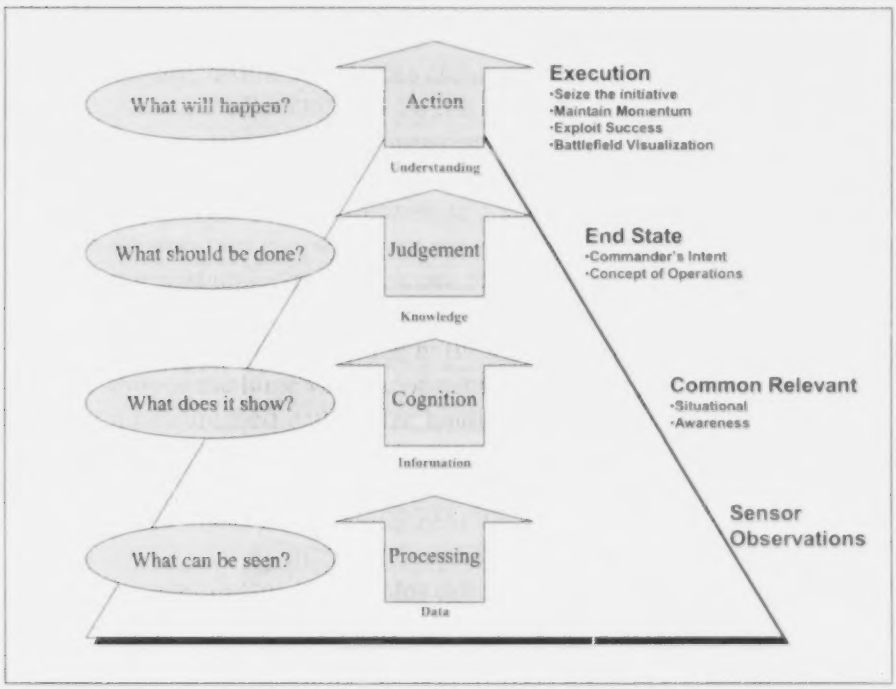

Figure 1-4-5: The Cognitive Hierarchy and the Art of Operations

25. Cognition transforms information into knowledge. Knowledge is the basis for key elements of operational design; the mission, the commander's intent, and the concept of operations. Because digitization introduces non-hierarchical linkages to an organisation, the commander

has an even greater obligation to clearly articulate these elements of the plan. Informed judgement transforms knowledge into understanding that allows units to seize the initiative, maintain momentum, and exploit success.

26. The process of deriving understanding from data, information and knowledge enables the commander to develop a relevant common picture throughout the force. To assist in this process, the commander designates the commander's critical information requirements (CCIR).

27. CCIR are an organising tool designed to focus the collection, reporting, and monitoring of information that is essential to accomplish the mission. This process is described in detail in Chapter 3. Critical information may come from friendly or neutral governmental or non-governmental organisations, the media, and politically oriented organisations. All of these can influence military operations, leadership perceptions, and the flow of information through information systems.

28. By focusing information technologies at the appropriate stages of the cognitive hierarchy we can enhance information superiority, support anticipatory planning and enable rapid execution. The areas for improvement include the ability to:

a. share vertically and horizontally a comprehensive and accurate relevant common picture;

b. rapidly disseminate planning guidance and newly generated options;

c. assess the viability of options;

d. calculate support and resource requirements and time-distance factors;

e. help visualise, illustrate, brief and rehearse options; and

f. increase the speed of analysis, compilation, and communication in order to leave more time for synthesis, which is the creative process of assigning meaning to information and generating potential options.

SECTION 5
INFORMATION MANAGEMENT

29. The dissemination and management of information is a command responsibility. Success or failure of the management of information lies within the command structure. While communications and information systems based on information technologies provide the means by which the information is processed, stored and disseminated, it is the information user who is ultimately responsible for the management of the information itself. Each participant in an operation is involved in the information management process and assumes responsibility for proper handling of the organisation's part of the Relevant Information.

30. The Army has transitioned from a time when the commander fought for information to a time when the commander is inundated with data, even before the fight for needed information begins. Information flow within the organisation is complex yet vital to the creation of a clear picture for the commander. Optimum information flow within the organisation requires both speed and clarity of transfer without creating an overabundance of fragmented or useless data. The organisation designs an information management plan to establish responsibilities and provide instructions on managing information. This plan is a *"scheme of manoeuvre"* for handling information within the organisation. The information management plan must be integrated and coordinated with the other elements of the commander's plan. With the increased information volume and flow experienced by commanders and staff the information management plan must not be treated as a secondary plan requiring a limited staff focus; it must become a primary element of the commander's plan with a dedicated staff focal point.

CHAPTER 2
FUNDAMENTALS, COMPONENTS AND ACTIVITIES

SECTION 1
INTRODUCTION

1. The aim of this chapter is to outline the nature of information and describe the fundamentals of Information Operations (IO). It serves to break the IO Combat Function into its component parts and describes the four critical activities essential in conducting IO. Integration of IO with the five other combat functions is essential to the production of Combat Power.

SECTION 2
FUNDAMENTALS

2. Information is defined as "processed and structured data of every description which may be used in operations." A given piece of data may be useable in itself but generally data must be processed (placed in context) and presented in a useable form for it to become information.

3. For information to become useful it must be evaluated. Information may be true or false, accurate or inaccurate, confirmed or unconfirmed, pertinent or not pertinent, and positive or negative. Information that has been evaluated becomes knowledge. When judgement is applied to knowledge we have understanding. Understanding is the basis for military plans.

4. IO "are continuous military operations within the Military Information Environment (MIE) that enable, enhance, and protect the commander's decision-action cycle and mission execution to achieve an information advantage across the full range of military operations. They include interacting with the Global Information Environment (GIE) and exploiting or attacking an adversary's information and decision systems."[3]

---

[3] B-GL-300-001/FP-000 *Conduct of Land Operations— Operational Level Doctrine for the Canadian Army*.

SECTION 3
COMPONENTS

5. The combat function of IO consists of six components broken into:

a. four support components:

(1) Communication Information Systems (CIS),

(2) Relevant Information, including intelligence, surveillance, target acquisition and reconnaissance (ISTAR),

(3) Civil-military Cooperation (CIMIC), and

(4) Public Affairs (PA); and

b. two action components:

(1) Offensive Information Operations (Off IO), and

(2) Defensive Information Operations (Def IO). (See Figure 2-3-1).

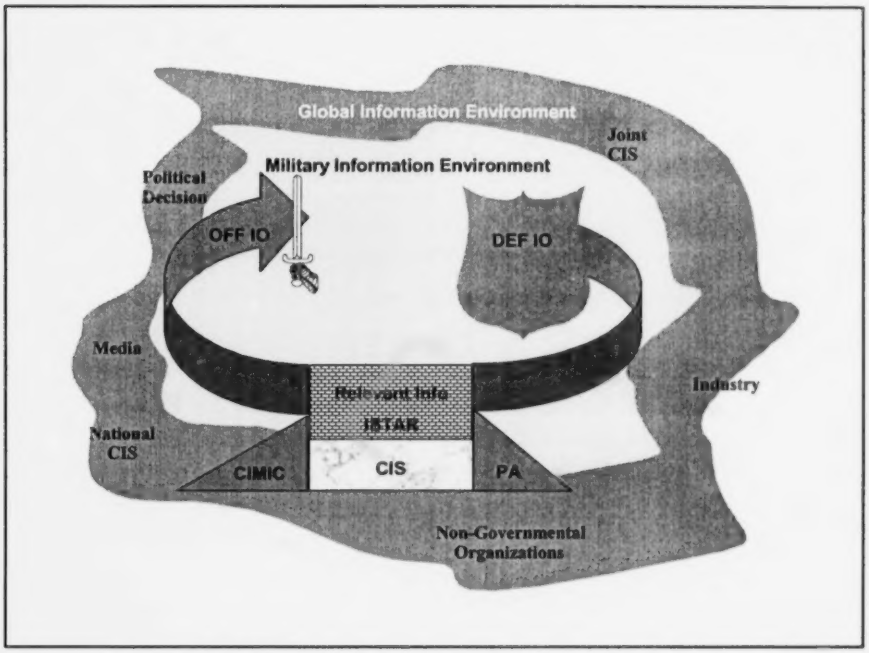

Figure 2-3-1: Global Information Environment

COMMUNICATION INFORMATION SYSTEMS

6. CIS collect, process, store, and disseminate information relating to current and future operations. Automation has made great advances in information processing, but human beings remain the most effective system for determining relevance and fusing information. CIS are those means that enable commanders and their staffs to:

a. manage information;

b. monitor the current situation;

c. integrate and coordinate operations across the combat functions;

d. coordinate joint, air and naval support;

e. update weapon systems targeting parameters; and

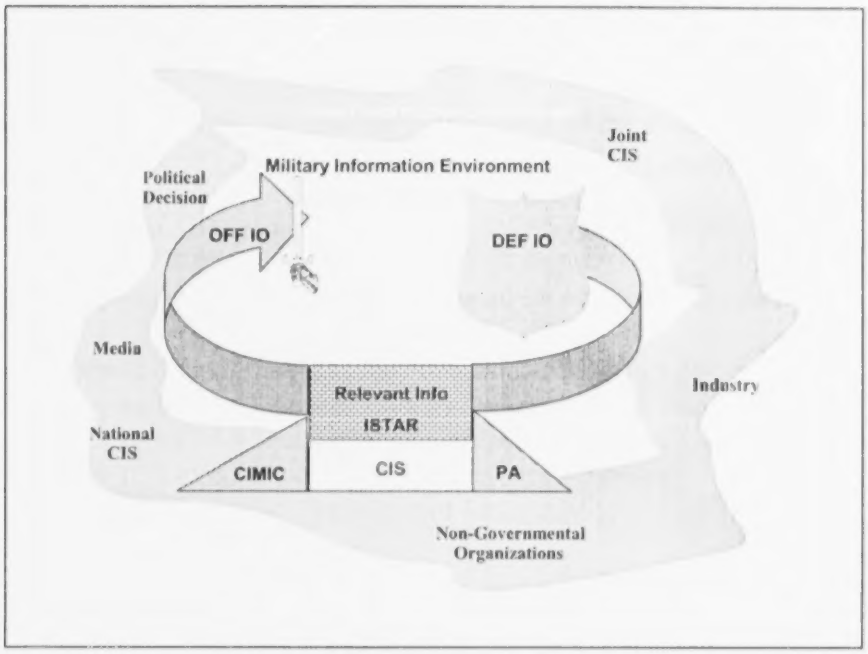

Figure 2-3-1: Global Information Environment

COMMUNICATION INFORMATION SYSTEMS

6. CIS collect, process, store, and disseminate information relating to current and future operations. Automation has made great advances in information processing, but human beings remain the most effective system for determining relevance and fusing information. CIS are those means that enable commanders and their staffs to:

a. manage information;

b. monitor the current situation;

c. integrate and coordinate operations across the combat functions;

d. coordinate joint, air and naval support;

e. update weapon systems targeting parameters; and

f. control close, deep and rear operations as one integrated operational framework.

ARCHITECTURE

7. CIS are essential to the effective application of military power. Of particular importance to CIS is the evolution of the Army's comprehensive command and information architecture with its three complementary architectural views focused on operational, system, and technical issues. The aim of this initiative is to create a common operating environment of standardized, interactive systems and templates for the collection, storage, and manipulation of all the information of the Army.

8. **Operational Architecture**. The operational architecture view of the overall command and information architecture establishes the required connectivity among processes, functions, information, and organizations to provide our command, control and information system (CCIS). It shows what we do, what information we need to do it, how often and with whom we need to exchange information and how we intend to manage our information holding.

9. **System Architecture**. The system architecture view of the overall command and information architecture seeks to identify relationships among Command and Control Information System (C2IS) components and create physical connectivity within the information system. It uses an organizational context to show system allocation and network structures and helps document engineering decisions, such as specific information protocols and bandwidth.

10. **Technical Architecture**. The technical architecture view of the overall command and information architecture establishes a set of rules governing the arrangement, interaction, and interdependence of all the parts and elements that together constitute our CIS. It specifies the permissible standards for designing CIS capabilities and is critical to the creation and maintenance of interactive systems.

INTEGRATION

11. The integration of CIS (both vertically and horizontally) facilitates tactical and operational agility, initiative, depth, synchronization, and versatility; this integration is essential to the success of the Army in joint and combined operations.

GLOBAL CONNECTIVITY

12. Global connectivity is essential for linking strategic, operational, and tactical aspects of IO and the ability to project forces worldwide. CIS support operations globally with space-based and terrain-based systems. CIS must be configured to provide the required information support with a minimum of physical repositioning, whether in a strategic deployment phase or moving for a tactical attack. Both military and commercial CIS play important roles in this architecture.

13. The Army uses information technologies on the battlefield to provide an integrated Command and Control structure. The Army is migrating from the current manual command and control system to a tiered common user core with associated specialist applications, which will function in a seamlessly fashion in garrison and in the field. This common user core concept uses Commercial Communication Services, Multinational Military Satellite Communications and the Tactical Command, Control and Communication System (TCCCS) as an information bearer. This common user core is supplemented as required by specialist applications to deal with specific information requirements or processing. The integration of modern CIS with our tactical units will continue to enhance their connectivity, decision-making, and, ultimately, lethality, survivability, and the ability to control the tempo of operations. Chapter 3 discusses the Army CIS.

14. Communications connectivity must allow for high-speed dissemination of information. This is achieved by providing a mix of hierarchical and broadcast communication. Hierarchical communication is well understood as it is the classical approach for military communications and is essential to disseminate information, which must follow a known processing path. Broadcast communication, which provides the ability to breakdown unnecessary organisational barrier therefore removing delays in dissemination of common and non-hierarchical information, is currently integrated to a lesser degree.

Broadcast communication provide the ability for direct down link of data or information from multiple sensors or databases to multiple echelons simultaneously and the broadcast of finished information products from theatre, departmental, or national agencies to deployed forces. Information can be provided on a push or pull mode to deployed forces.

INFORMATION MANAGEMENT

15. The need to manage information is not new; however, the volume and the diverse types of information that must be managed to ensure successful operations are increasing exponentially. To be successful in managing information we must approach information of all types, forms and purpose in a holistic fashion. Our goal must be to minimize duplication of information and efforts, and the loss of information, while maximizing information quality and timeliness, information integrity, and access speed. Information management is discussed in more details in B-GL-331-001/FP-001, *Command Support Doctrine*.

RELEVANT INFORMATION

16. Commanders have struggled with how to best capitalize on available information throughout the history of warfare. The drive to know as much as possible about their own forces location, combat effectiveness, current activity and the enemy's location, disposition, combat effectiveness, intended actions, has been a durable characteristic of successful commanders, regardless of the time period or nationality. Today, commanders operate in an environment marked by a massive increase in the quantity of information, with the associated ability to rapidly collect and move information and decisions. These decisions and information can have an immediate impact at the strategic, operational or tactical levels regardless of point or level of origin. The explosive expansion of the MIE has made military operations more dependent than ever before on non-military individuals, organizations and systems. These dependencies have made a commander's MIE more vulnerable than ever before to an adversary.

17. The collection, use and dissemination of Relevant Information are based upon the systematic integration and co-ordination of information regardless of the source or means of collection. Relevant

Information are fused in order to provide the commander with a thorough understanding of the present situation and assist him in understanding what his future Area of Operations (AO) will look like. When shared throughout the force, this common understanding of the situation contributes to cohesion and allows subordinates to understand clearly the commander's intent and therefore, the main effort. This is critical to the Canadian Army's philosophy of Mission Command.

18. Relevant Information includes all information in a commander's MIE. It includes friendly information collected in response to the commander's Friendly Force Information Requirements, higher commander's intent and concept of operations, and various other groups in the conflict (their political military leaders, motives, traditions, institutions, culture, language and histories). Intelligence is the special subset of Relevant Information that deals with the adversary (or potential adversary), weather and terrain. Intelligence takes on increased, even crucial, importance in the Information Age. Because IO gives the AO global connectivity, intelligence on current or potential adversaries must be prepared on a global scale. Interaction with the MIE requires timely intelligence about many aspects of current or potential adversaries, to include cultural, political, and commercial aspects.

19. Commanders must have information to command. Information allows the commander's decision-action cycle to function and gives direction to the forces to accomplish their operational missions. The collection, processing, and dissemination of information are key to achieving situational awareness throughout the force, which creates the opportunity for unity of effort toward mission accomplishment. The commander operates within the GIE, adjusting his MIE to enhance his situational awareness as appropriate for the operation at hand.

20. B-GL-300-003/FP-000, *Command*, Chapter 3, Annex A, lists a range of commander's Information Requirements. Commanders determine the critical information for each operation and publish those requirements as their commander's Critical Information Requirements (CCIR). The commander alone can decide what information is critical based on the mission, experience, and the higher echelon commander's intent. The staff may only recommend CCIR to the commander as:

a. Priority Intelligence Requirements (PIR) to determine what the commander wants or needs to know about the enemy, his purpose, and/or terrain (how I see the enemy).

b. Friendly Forces Information Requirements (FFIR) to allow the commander to determine the combat capabilities of his or adjacent friendly units (how I see myself).

c. Essential Elements of Friendly Information (EEFI) to allow the commander to determine how he must protect the force from the enemy's information-gathering systems (how can I prevent the enemy from seeing me).

21. A key to successful operations is an accurate Intelligence Preparation of the Battlefield (IPB) focused on the MIE. Relevant Information, including intelligence gathering and support to operations begins in peacetime and must be continuous throughout all phases of an operation or campaign. Advances in information technology are making it possible to change how information is provided in support of operations.

22. Successful IO requires the fusion of information from a variety of sources. Advances in sensors, processors, and communications are combined to provide detailed, timely reconnaissance and surveillance of almost any place on the globe. Both military and non-military sources provide information that can be used to produce information and intelligence. Open-source information and intelligence or reporting will provide a great deal of the order of battle (ORBAT) and technical data. Successful integration of IO also requires an IPB grounded in a thorough understanding of an adversary's capabilities and decision-making style. Relevant Information as a component of IO is addressed in detail in Chapter 4.

23. Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) is the process by which a commander does his own focused information gathering as an integral part of Relevant Information. In the modern environment the differentiation between type of sensors and who controls them is becoming less important. It is the information that matters. A single sensor can be simultaneously gathering a wide range of information for many users without degradation to the needs of the primary user. ISTAR is described in detail in Chapter 5.

PUBLIC AFFAIRS

24. In our recent history, success or failure of military operations has been influenced greatly by whether the public believed the mission was successful. The Army has been less than successful in PA and this has had a derogatory effect on the Canadian Forces reputation and operational effectiveness. Most military operations are conducted under the full glare of public scrutiny. National and international news media coverage plays a major role in quickly forming public debate and shaping public opinion. The news media serve as a public forum for the analysis and critique of goals, objectives, and actions. It can effect political, strategic, and operational planning, decisions, and mission success or failure.

25. The reality of near real-time information, processed and transmitted at greater speeds and to wider audiences than in the past, has bridged the gap between what occurs on the ground and the goals and objectives from the national level. PA is a commander's responsibility. The public affairs officer (PAO) assist the commander in monitoring public perceptions, and developing and disseminating clear and objective messages about military operations in line with the commander's intent. The objective of PA is to help ensure information superiority by seizing the initiative with respect to media activities and putting in place programs which:

a. Protect soldiers from the effects of an adversary propaganda, misinformation and rumour. Well-informed soldiers are effective soldiers.

b. Support open, independent reporting and access to units and soldiers.

c. Establish the conditions leading to confidence in the Army.

d. Provide a balanced, fair and credible presentation of information that communicates the Army's story through an expedited flow of complete, accurate and timely information to the public in the AO, Canada and the world.

26. Commanders use their internal information programmes to inform soldiers about where they fit in, what is expected of them, and how

they help accomplish the mission. This information also helps soldiers combat the effects of enemy propaganda or misinformation. Commanders, through their PAO, initiate, direct, and emphasize internal information topics and programs. Every soldier must receive information specific to the operation through command channels and world, national, and local news. The media are an important information channel to the public; however commanders, staff officers, and soldiers must balance OPSEC and other operational requirements when working with the media.

27. PA personnel support commanders by assessing the information environment and advising them on the PA implications of current and future operations, and by disseminating the PA plan in support of these operations. Commanders understand the importance of achieving a balanced, fair, and credible presentation of information to both internal and external audiences. Commanders integrate PA into their decision-making process by considering it in their assessment of the situation and development of courses of actions, plans, and orders. Further information regarding PA is contained in Chapter 7.

CIVIL-MILITARY COOPERATION

28. CIMIC provides the interface with critical actors and influences in the GIE. Whether in peace, conflict, or war, the conduct of a successful operation often depends on CIMIC support, in some case CIMIC may even be the main effort. Although conditions differ across the spectrum of conflict, CIMIC activities establish, maintain, influence, or exploit relations among military forces, civil authorities, and the civilian populace in an AO to facilitate operations.

29. The CIMIC Staffs will be required to interact with key actors and influences in the GIE, such as NGOs and local authorities. CIMIC elements support military operations by applying their skills and experience in host nation support public administration, economics, public facilities, linguistics, cultural affairs, and civil information and by collecting information relevant to the CCIRs. CIMIC personnel have an intricate and important role in providing information for both the intelligence cycle and the operation planning cycle. Additional information on CIMIC is contained in Chapter 8.

OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS

30. The complexity and range of today's MIE increase the difficulty of achieving a comprehensive disruption of an adversary's capabilities through any single attack or application of combat power. This places a premium upon the effective integration and co-ordination of IO actions to achieve maximum results when launching attacks. Likewise, careful integration is also required to protect our critical systems and processes from adversary attacks. Without the complete and thorough integration and co-ordination of Off IO and Def IO, operational effectiveness will be reduced and potential vulnerabilities exposed.

OFFENSIVE INFORMATION OPERATIONS

31. The goal of Off IO is to gain control over our adversary's command function and influence enemy and neutral persons, both in terms of flow of information and level of Situational Awareness (SA). With effective Off IO, we can either prevent an adversary from exercising effective Command and Control (C2) or leverage its beliefs to our advantage.

32. Off IO can strike at the adversary's capabilities at all echelons, targeting personnel, equipment, communications, and facilities in an effort to disrupt or shape adversary operations. Relevant Information, including ISTAR plays a key role in Off IO planning and operations, with the creation and maintenance of regional databases on personal, historical, and cultural influences, IPB, and Battle Damage Assessments (BDA): both soft and hard kills. The principal Off IO approach for influencing the adversary is the co-ordinated application of the four information activities described in Section 4 of this Chapter.

DEFENSIVE INFORMATION OPERATIONS

33. Def IO seeks to maintain effective C2 of friendly forces by negating or turning to a friendly advantage the adversary's efforts to influence, degrade, or destroy friendly C2 systems, while protecting our soldiers, the neutral population and our own national population against the effects of enemy Off IO actions. Def IO is divided into active and passive measures and seeks to limit the vulnerability of forces (personnel, equipment, and information) to hostile action, even as deployed forces

face ever-expanding threats and adversary capabilities. Def IO includes countering an adversary's propaganda and Psychological Operations (PSYOPS) to prevent them from affecting friendly operations, options, public opinion, and the morale of friendly troops.

SECTION 4
ACTIVITIES

34. IO involves acquiring, using, protecting and denying information. When effectively executed, these critical activities supplement the human skills of mission command, speed decision-making, minimize uncertainty, focus combat power, provide force protection, harness organizational capabilities, link the MIE to the GIE, and enhance SA. These activities apply to both information and CIS (hardware, people, organizations, and processes). Although listed sequentially, these activities are concurrent and seamless in their application (see Figure 2-4-2).

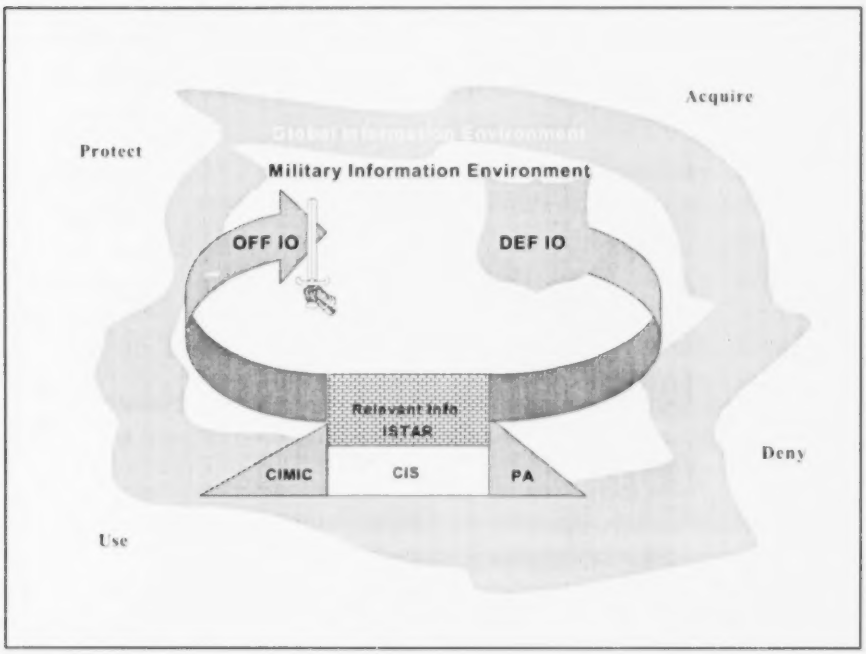

Figure 2-4-2: Information Operations Activities

face ever-expanding threats and adversary capabilities. Def IO includes countering an adversary's propaganda and Psychological Operations (PSYOPS) to prevent them from affecting friendly operations, options, public opinion, and the morale of friendly troops.

SECTION 4
ACTIVITIES

34. IO involves acquiring, using, protecting and denying information. When effectively executed, these critical activities supplement the human skills of mission command, speed decision-making, minimize uncertainty, focus combat power, provide force protection, harness organizational capabilities, link the MIE to the GIE, and enhance SA. These activities apply to both information and CIS (hardware, people, organizations, and processes). Although listed sequentially, these activities are concurrent and seamless in their application (see Figure 2-4-2).

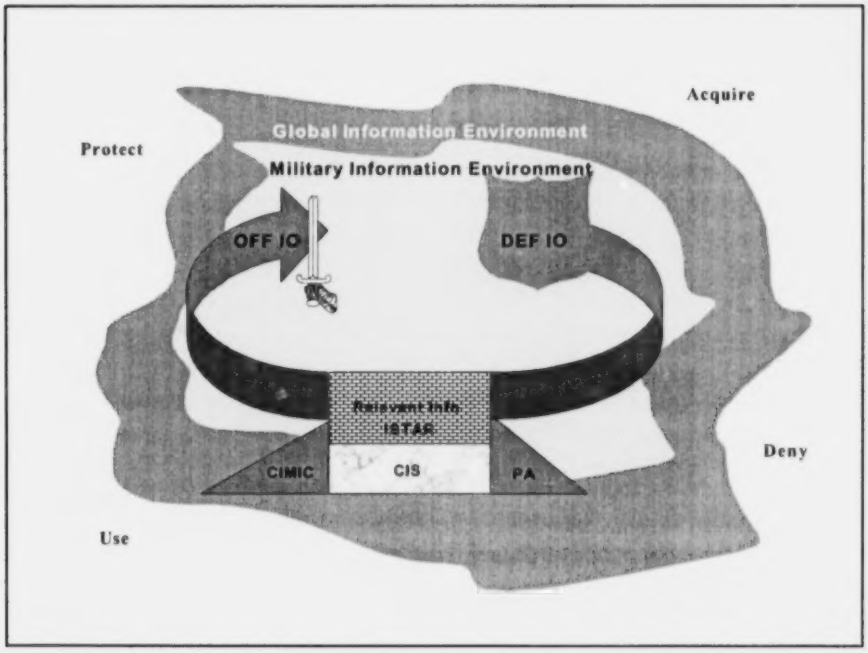

Figure 2-4-2: Information Operations Activities

ACQUIRE

35. Commanders must consider the nature of the information required before allocating resources to acquire it. Initial questions include:

a. What do I already know?

b. What information is needed?

c. What is the nature of that information?

d. How can that information be acquired?

36. The CCIRs will normally be formulated as part of the commander's estimate and articulated in Orders. Information is also acquired using a more general information collection cycle focusing on gathering Relevant Information from other sources and influences in the MIE. The information needs of the commander are not answered by a single source, but by:

a. a combination of his own ISTAR systems;

b. unit situational updates;

c. human intelligence (HUMINT) activities;

d. strategic or national agencies (Intelligence, External affairs etc);

e. interface with local populations, police forces and news media; and

f. GIE.

USE

37. Commanders in the future will have access to an unprecedented amount of information. In the past the problem for commanders was acquiring information that was timely and accurate. The problem facing the modern commander is information overload. Using information

means exploiting, analyzing, verifying, updating and managing (moving, storing and presenting) information. The result is common SA and the knowledge necessary to plan for future operations. The commander is able to see his AO through the use of space, air, and ground systems to acquire Relevant Information and provide a current situation. The commander expands his thinking to include all CIS and organizations accessible in the GIE. Once the data is acquired, analyzed, and collated, the information is used to update and validate a common SA. This common SA provides the basis to refine, continue, or adjust decisions, plans, and operations:

a. Information is focused and used by issuing guidance, prioritizing assets, and establishing requirements.

b. Staffs then refine the guidance into operational plans or Operation Orders. They seek to integrate information at all echelons and plan the use of all available information, regardless of the source.

38. The most timely, accurate, or Relevant Information, particularly in Operations other than War (OOTW), may come from sources outside the unit or military channels. A unit must make use of both organic and non-organic CIS. Non-organic systems are either governmental or non-governmental (GIE). Use of other governmental systems, (DND and non-DND) is co-ordinated by NDHQ. Using systems outside the government is more complex. Units can use some services openly and passively, such as listening to, or subscribing to, broadcast media. Units can also make overt use of services such as communications relays or weather forecasting. However, commanders must be aware of the legal and policy limits on their use of any non-DND CIS.

39. How the information nets within an organization are linked together can provide multiple conduits for information. Horizontal inter-netting of CIS at the lowest possible levels provides a deeper, multidimensional picture than traditional, stovepipe reporting.

EXPLOIT

40. Exploitation is described as "*taking full advantage of any information that has come to hand for military operational purposes.*" All information environments and systems surrounding an operation,

friendly and adversarial, military and non-military, must be thought of as information to be exploited. Exploitation of information needs to be considered in a general way and not just from an intelligence point of view. All information acquired need exploitation which involves:

a. analysis of information;

b. access to database support;

c. access to CIS both military and global;

d. verification and updating of information; and

e. presentation of information in a useable format.

41. Information collected on an adversary after being processed becomes intelligence. Intelligence by its nature and the means by which it has been acquired is sensitive and requires special protection. Information gathering and intelligence work must begin in peacetime to establish the analysis of the AO and how potential adversaries operate. Knowledge of the adversary's information infrastructure is as important as knowledge of a potential adversary's strategies, tactics, techniques, and procedures. Knowledge of the adversary's infrastructure will lead to assessment of personnel, facilities, sensors, processors, and decision-making process. The assessment asks the question: "How reliant is the adversary on the GIE for information?" This in turn affects how friendly forces will interacts with the GIE, to include the media, government agencies, NGOs, and foreign governments. Intelligence gained through exploitation supports IO planning and operations, especially deception, PSYOPS, and physical destruction. (These capabilities are described in Chapter 6.)

VERIFY

42. Information must be checked for accuracy. In the past, our thought has been more on verification of intelligence. Now verification of all information is critical. Information is perishable and requires constant updating to remain relevant. Events can make an item of information irrelevant or so unrepresentative as to portray a highly inaccurate picture of reality. Information beyond a certain age will detract from the commander's SA and may impede his ability to visualize the battlefield. Standard Operating Procedures (SOPs), CCIRs, and plans(both

operational and collection plans) must all be sensitive to the perishability of information. Moreover, from a technical perspective, CIS managers must respond by managing the systems and information to enable assured and timely communication and decision-making.

MANAGE

43. In order to conduct operations, information requires careful coordination and synchronization. With guidance issued, the staff coordinates and integrates information requirements to co-ordinate the critical information flow with the operational concept. Managing information must focus on the operational requirement that will derive information from the Operational Planning Process (OPP), ISTAR systems, Counter-Intelligence (CI), Operational Security (OPSEC), communications, and security operations. Managing information includes: managing paper based systems and the electromagnetic (EM) spectrum; deciding what sources and systems to use; ensuring a reliable flow of information (horizontal and vertical integration), data access and integrity; and resolving differences among information from multiple sources. This planning must be an integral part of operations planning and in many cases precedes a decision on a scheme of manoeuvre or fire support and definitely precedes mission execution.

44. Effective management of information and assets allows information to flow horizontally and vertically across all combat functions to enable effective planning, preparation, decision-making, and execution. This serves to eliminate duplicated efforts and unnecessary redundancy, allowing systems to deal with time-sensitive, Relevant Information. The keys to these effective communication and information flows are connectivity, throughput, and resilience. Units can manage connectivity among their organic assets. The difficulty comes in maintaining horizontal and vertical connectivity outside the unit, particularly when dealing with forces using older voice-based and paper-based systems or different communications and CIS. Connectivity is accomplished through the maintenance of electronic and human links vertically and laterally outside the unit. When dealing with forces or units less technically capable, teams must be prepared to deploy with specialists or liaison personnel equipped with the necessary equipment.

45. Resilience is the ability of CIS, from a technical and management perspective, to provide the necessary connectivity and

continuity when CIS are degraded. Additionally, Army leaders and planners must understand how military information and systems interconnect and interact with the GIE. Over reliance on commercial systems, particularly satellites and host nation telecommunications networks, may impose restrictions or limitations. Close management and consistent co-ordination will help assure the availability, reliability, and timeliness of command support systems.

PROTECT

46. While the proliferation of information and information technology can be a great advantage, it is also a potentially significant risk that must be accounted for in every operation. Protection of soldiers and equipment, although not new, has increased in importance in today's information-rich environment. Friendly information and CIS must be protected throughout the AO. Operationally, protecting information requires viewing friendly vulnerabilities from the enemy's Off IO perspective. Commanders must examine the vulnerability of their soldiers and systems to exploitation or attack by an enemy capable of attacking friendly C2 and personnel on a wide front by employing Electronic Warfare (EW), physical destruction, deception, and misinformation.

47. In order to stop or delay a weapon or system from functioning, an adversary might attack the information or CIS that enable that system. For example, an adversary might introduce a malicious software code through a communications network directly into the CIS to disrupt the sharing and distribution of combat information with other Army and joint systems. Actions taken to protect the capability to operate unconstrained in the MIE are considered part of Def IO.

48. Relevant Information and the supporting CIS must be protected at the electronic, physical, and human levels, in relation to the potential threat—all without impeding the overall operation. Security programs that identify threats to Command and Command Support systems also take on increased importance while in garrison because the porous and open nature of the GIE makes the Command Support information infrastructure vulnerable to attack or exploitation at any time. As part of planning for both deployed and garrison operations, commanders at all levels must analyze the unit's information structure to identify critical vulnerabilities and provide the necessary protection. Everything cannot be protected. Therefore, commanders must perform a risk management

analysis to identify essential information and CIS that must be kept free from disruption or corruption. This will also lead to OPSEC priorities.

49. Elements of the infrastructure to be protected are data, computers, communications systems, and support facilities. Planners must integrate elements of the GIE into plans to ensure that commanders consider their impact, or potential impact in any operation. An assessment and vulnerability analysis must provide the timely and accurate data needed to identify and target threats and potential threats to friendly CIS.

50. Protecting computer and communications systems from enemy intrusion, disruption, and destruction is an initial basic step in an overall protection approach. However, commanders must also be sensitive to enemy attempts at deception and propaganda. A resourceful enemy may employ propaganda to predispose a commander and his staff toward a specific course of action and then exploit that mindset with a deception operation. IO may often take place under degraded conditions. Besides adversary or accidental actions, natural phenomena may degrade or disrupt equipment or services. Because of the complexity and fragility of CIS, the plans of a unit should include procedures for operating with degraded CIS.

DENY

51. Off IO make possible the goal of attacking an adversary simultaneously at all levels with overwhelming force. Off IO are intended to prevent an adversary from exercising effective C2 and maintain cohesion of his forces by denying the adversary information or influencing, degrading, or destroying the adversary's information and CIS.

52. IO give the commander the means to attack an adversary throughout the depth of the AO, far beyond the range of direct or indirect fire systems. The goal is to degrade the adversary's confidence in either his data or his ability to command and control operations. By attacking or confusing his sense of the battlefield, friendly forces gain information dominance and a subsequent relative advantage in applying combat power or controlling a situation. Using Off IO to gain information superiority is critical to supporting our manoeuvrist approach to operations.

53. Information denial generally requires time and occurs over relatively large areas. To blind or deafen an adversary requires that most of his major ISTAR systems be influenced or engaged. Therefore, attacks of adversary CIS are normally planned as a series of engagements, contributing to a larger operation or higher objective.

54. All levels of command may not have the required assets to perform all Off IO missions, particularly those involving deception and PSYOPS. However, the value in denying an adversary effective command or influencing the beliefs of his troops and population in the AO remains important and commanders at all levels need to be prepared to contribute to achieving that objective. Multiple attack options in IO will result from analysis and assessment of potential targets. Generally, the earlier an adversary's decision-making cycle is disrupted, the greater the effect it can have on his capabilities. It is often more effective to disrupt the adversary's early sensing or decision-making processes rather than trying to disrupt execution of a decision already made. Operational commanders must weigh the relative advantages to be gained by attacking adversary C2 nodes against the potential loss of intelligence from adversary signatures, radiation, or emissions and the need to protect intelligence methods and sources.

SECTION 5
INTEGRATION WITH OTHER COMBAT FUNCTIONS

COMMAND

55. IO directly support the command function. IO provide the necessary information for the commander's decision-action cycle and co-ordinate all aspects of information. The very nature of IO is to assist the commander in defeating an adversary by preserving his decision-action cycle while degrading the adversary's ability to achieve information superiority. IO alone may or may not allow a commander to defeat an adversary.

PROTECTION

56. The Def IO is clearly a significant contributor to protection and must therefore be integrated in the planning process. In the IO context, protection means dealing with the protection of information, processes,

systems and sources to ensure a commander has freedom of action. Def IO takes many forms such as electronic protection of information systems, protection of sources of information, and physical protection of both equipment and personnel (commanders). The amount of protection that is necessary is dependent on the threat capabilities to gather and exploit our information (his ISTAR systems). It must be realised that all information cannot be protected from a determined adversary. An intelligence estimate of friendly vulnerabilities is key to providing sufficient protection without affecting a commander's flexibility. Def IO must be integrated by IO specialists into the overall protection plan in accordance with
Chapter 6 of B-GL-300-006/FP-001, *Land Force Protection*.

FIREPOWER

57. Firepower of all types is dependent on the quality and timeliness of targeting information. IO provide the sensors, analysis and information flow necessary to engage a target and determine how successful the engagement was. Targets must now not only be thought of in physical terms but in terms of processes, human interactions (such as moral cohesion) and temporary effects. The targeting process links IO (and its elements such as ISTAR and Command and Control Warfare (C2W)) to firepower. Off IO must be integrated in the targeting process. The IO specialist can nominate targets, however, the commander must still decide the priority of effort and the resource allocation. The targeting process is discussed in details in Chapter 4 of B-GL-300-007/FP-001, *Land Force Firepower*.

MANOEUVRE

58. IO identify the weaknesses and provide the information to the manoeuvre commander so the right forces can be brought to bear at the right place and right time. IO provide the SA necessary for a commander to fight and plan for future operations.

SUSTAINMENT

59. To sustain forces, information is critical. SA and Asset Visibility for all units in a formation is critical to "just in time" re-supply.

Sustainment troops will require specific types of databases and access to national stocks in order to predict sustainment levels. The information systems will need to be robust and will need protection. Since sustainment must extend from the deployed troops to national/strategic level, it is extremely vulnerable to disruption through IO.

CHAPTER 3
COMMUNICATION AND INFORMATION SYSTEMS

Definition-Assembly of equipment, methods and procedures, and if necessary personnel, organised so as to accomplishspecific information conveyance and processing functions.

(NATO def AcomP-1, Oct 94)

SECTION 1
THE ENVIRONMENT

1. Rapidly advancing information-based technologies and an increasingly competitive global environment have thrust information into centre stage in society, government and warfare. All technological revolutions of this century pale in comparison with the spectacular revolution in solid state electronics over the past three decades—the likes of which have never been seen before in human history. The microchip has generated a phenomenal revolution in information. Storage and processing of information and information-based technologies are pervasive and impact on every facet of warfighting: from the planning, the deployment, and the sustainment process to the plethora of weapons systems employed by land, air and maritime forces.

2. This increased use breeds dependence as can be seen by the chart in Figure 3-1-1. The rise in the 20th century is almost vertical. Timely, accurate, and Relevant Information is absolutely essential for combat, as large force structures give way to smaller, highly trained and technically equipped forces.

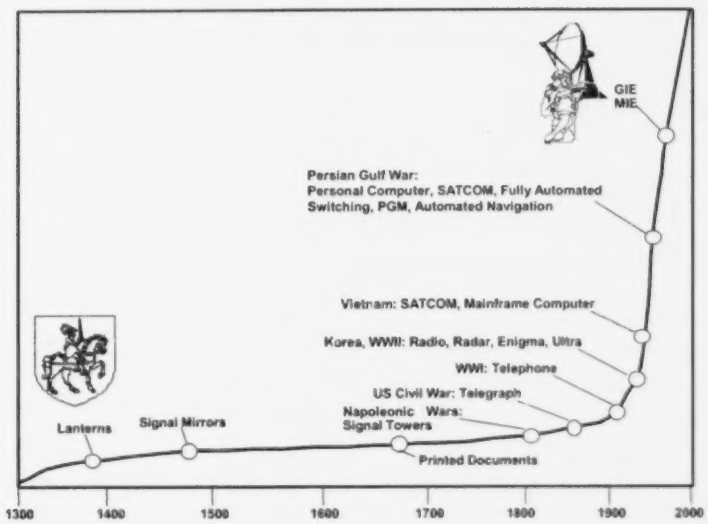

Figure 3-1-1: Increasing Speed in Flow & Processing of Information Throughout the Ages

3. Information itself is a global resource, vital to national security. Increasingly complex information systems are being integrated into traditional disciplines such as mobility, logistics, firepower, and communications. These systems are designed and employed with inherent vulnerabilities that are in many cases the unavoidable consequence of enhanced functionality, efficiency and convenience to users. The relative low cost associated with such technology makes it efficient and cost effective to extend the capabilities (and vulnerabilities) to an unprecedented number of users. The broad access to and use of these information systems enhances warfighting. However, these useful capabilities induce dependence, and that dependence creates vulnerabilities. These vulnerabilities are a double edged-sword— on one hand representing areas that the Land Force must protect while on the other hand creating new opportunities that can be exploited against adversaries.

SECTION 2
FUNCTIONS

4. Land Force Communication and Information System (CIS) will support operations by providing the integrated digital information network necessary to achieve the commander's goal of information superiority on the battlefield. These systems support the staff processes and allow the

sharing of information on an all-informed basis to support mutual understanding and promote unity of effort. The Land Force must be capable of operating as part of a joint, multinational force and hence will require a high degree of interoperability from its CIS. The Land Force system must also provide reliable connectivity in the tactical and infrastructure environments, including interfaces with co-operating forces and infrastructure to enable the acquisition, processing, and distribution of information necessary to ensure the successful execution of the commander's mission. There is also a need to ensure a complementary level of functional interoperability between sensor platforms, communication networks and related information systems. In order to achieve this required degree of interoperability the Land Force must establish architectural control by defining the interoperability requirements, establishing technical interoperability standards, and mandating system integration guidelines.

5. The required functionality, and levels of interoperability will be achieved by the application of current and evolving technologies. Digital technologies provide the means to better exploit information, thereby providing an information advantage on the future battlefield. Digital technologies are applied to support the acquisition (e.g. sensor systems), distribution (e.g. communications), and processing (e.g. information systems) of information. Some other technologies that will provide improve functionality are data compression techniques, advanced network technologies, and multilevel security concepts. These technologies will be integrated to provide the Land Force with a seamless, interoperable digital network extending across the various functions on the battlefield and garrison up through the levels of operations to the National strategic level. The rapid pace of information technology development will be tempered by the fiscal realities and priorities of the Land Force. This may mean that the Land Force will introduce these technologies and capabilities through an evolutionary acquisition process, taking advantage of allied developments, making use of commercial off-the-shelf (COTS), government off-the-shelf (GOTS) and military off-the-shelf (MOTS) technology and products.

6. This evolutionary acquisition process while meeting fiscal realities and priorities of the Land Force could result in potential asymmetrical capabilities which will need to be carefully factored into any assessment of capability. As well in any deployment or action, the Land Force must assume that adversaries may have at least some types of advanced weaponry, even if that weapon is a computer connected to the Internet. An adversary may also have some niche, information-based

technologies or capabilities that will present the Land Force with an asymmetric challenge.

SECTION 3
ROLE

7. The role of CIS is to provide the infrastructure that allows the Land Force to operate within the MIE and interface with the GIE. CIS are used to enable the integration of all activities. The major roles of CIS are to:

a. support the decision-making process;

b. transmit information, including orders and reports;

c. link sensors, commanders and shooters;

d. provide a multi-dimensional relevant common picture; and

e. enable efficient sustainment of the force.

8. The accelerated development of information technologies has created new techniques for managing, transporting, processing, and presenting data. The scope of these techniques encompasses imagery, video, colour graphics, digital overlays, geospatial information and database technology. With this revolution of information technology, developments in satellite communications, network and computer technology combined with complimentary non-military developments the commander has a potential for global reach. CIS architecture should allow for force tailoring during any phase of an operation. Operations take place in a global environment and entail information from a host of information sources. Military and non-military systems will provide this global capability and support commanders across the full range of operations. (see Figure 3-3-2).

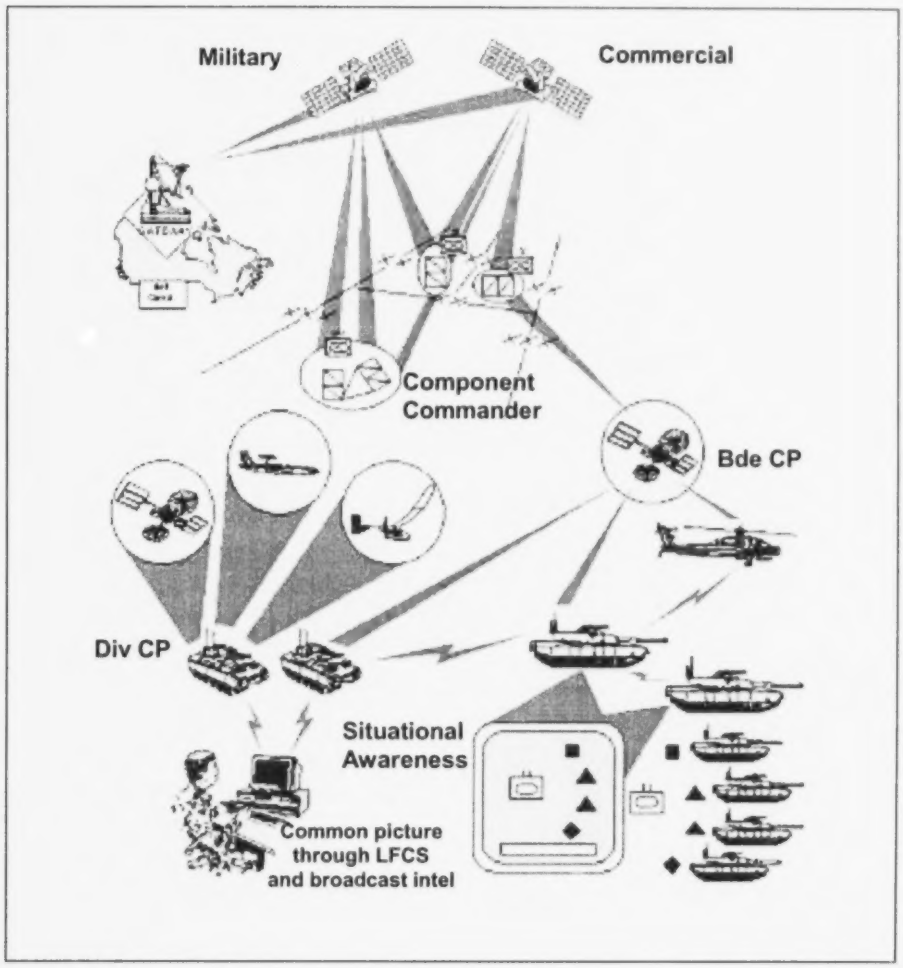

Figure 3-3-2: Global Communications Network

(A Representative Structure Combining Canadian Military/Commercial and Allied Military Systems)

SECTION 4
MILITARY INFORMATION SYSTEMS

9. CIS integrate fielded and developmental battlefield automation systems and communications to functionally link strategic, operational, and tactical headquarters. CIS maximise available information networks through near seamless connectivity and interoperability.

10. LF CCIS is defined as "*An integrated system comprised of doctrine, procedures, organizational structure, personnel, equipment,*

facilities, and communications which provide authorities at all levels with timely and adequate data to plan, direct and control their activities." In its broadest sense, it comprises: Information Management (IM) which is the policy, planning, and strategy aspect; Information Systems (IS) which are the procedural aspects and equipment which has two elements: firstly non-automated equipment e.g., records, files, books; and secondly, Information Technology (IT) which is the automated portion and consists of applications, infrastructure and databases.

11. The architecture of the Land Force Command and control Information System (LFC2IS) supports the Land Force Command and Control System (LFCCS). This system architecture envisions a three tiered approach to interoperability. Figure 3-4-3 illustrates this architecture. The respective information systems are integrated into a common user core (CUC) for garrison and field operations. It also provides for interoperability between joint and multinational forces as well. The bottom tier can be thought of as the foundation that supports the rest of the strategy, comprising the digital information distribution backbone and position determination and navigation capability. The middle tier is the CUC which provides common applications and services such as, command and control tools, digital geospatial services, database management, planning, orders preparation and messaging. This CUC is tailored to the user requirement. The top tier houses specialized and functional applications (Apps) used to supplement the CUC functionality. These are applications and not systems on their own as they use the CUC for their core functionality.

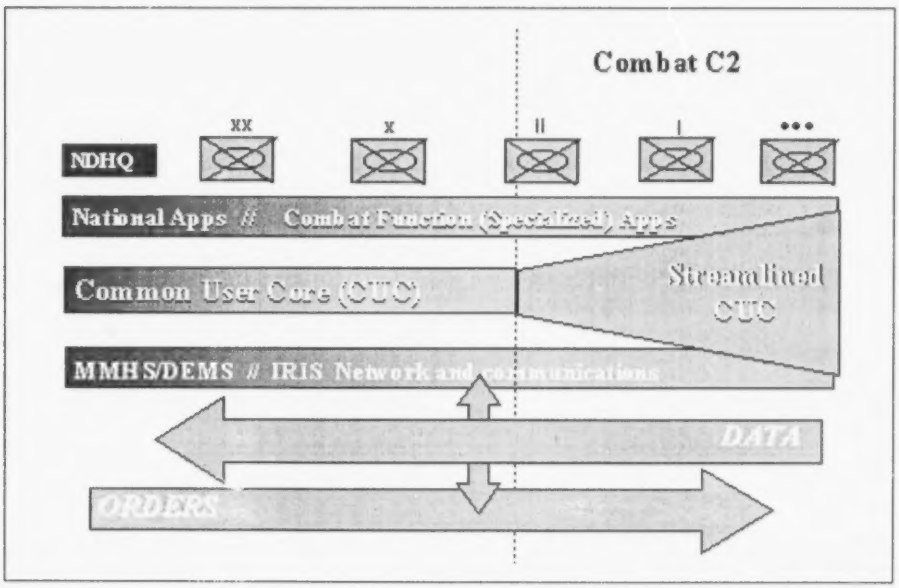

Figure 3-4-3: Land Force Communication Information Systems

SECTION 5
NON-MILITARY INFORMATION SYSTEMS

12. Information technology is growing exponentially and transforming how the world conducts business, diplomacy and war. This means that commanders must have a much broader and externally oriented view of all sources of information systems when executing Information Operations (IO). The conundrum is that the Land Force has limited authority for securing civilian infrastructure or influencing the content of its products. Technological improvements in mobility, digitization, weapons, and sensors continue to reduce factors of time and space and demands faster tempos of operations across much greater areas.

13. Increasing global population, rapidly expanding world economic markets, and unprecedented advances in information systems technology are creating a global explosion of information networks of a non-military or commercial nature. These ever-increasing networks are rapidly creating a global web or infosphere. The global nature and speed of new broadcasts can elevate apparently obscure news into international spectacles. The rapidly growing number of players in the GIE share new information over networks at a steadily increasing rate.

14. Cellular communications and data compression advances increasingly provide greater communications freedom to individuals in ever wider regions of the globe. These advances enable individual soldiers as well as media or others to independently reach home using the Internet or broadcast and publication sources. Potential sources of immediate information and the number and variety of MIE influences (both intentional and inadvertent) are rapidly multiplying. The cumulative effects of these changes permanently alter the shape of organisations and CCIS architectures in ways that are just becoming evident. Some examples of this are: networks in some areas supplanting traditional hierarchies as the major organising concept; in the commercial world eliminating much of the status-monitoring functions, and new ways of thinking and operating as elements relatively low in the organisation now have information to make and execute decisions. The Army has traditionally relied on a hierarchical approach to command and manage information. The advances in commercial technologies is making it possible to share large amounts of Relevant Information in a non-hierarchical manner while retaining the hierarchical path for critical information directly associated with hierarchical information processing.

15. Much of the Land Force information traffic flows over commercial systems. This is quite true domestically and like most nations the Land Force relies on elements of an information environment it does not control. Some examples of non-military IS are:

a. Canadian and host nation Public Switched Networks (PSNs) and postal and telegraph systems;

b. commercial communications satellites such as INTELSAT and INMARSAT;

c. commercial, international news media; and

d. public-accessed databases and bulletin boards.

16. While the availability of non-military IS can often offer commanders an alternative means to satisfy requirements there is a need to carefully assess the security risks of this option. Using non-military IS may also reduce the requirement for deployed military IS, and allow planners to compensate for shortages and or meet surge requirements in this area. Additionally, there may be savings in support and maintenance in using non-military IS.

SECTION 6
PLANNING OF COMMUNICATION AND INFORMATION SYSTEMS

NON-MILITARY INFORMATION SYSTEMS

17. The G6 is responsible for standardisation of non-military equipment and software used throughout the AO. Planners who deploy modular IS will need to ensure that these systems ideally are open, non-proprietary, and have commonly accepted standards and protocols in order to simplify the interface requirements.

TRAINING

18. Users will be challenged by the digitization of the battlefield, by interface requirements between operators and the system, and by the need

to develop effective training strategies. The optimal use of IS will depend on the availability of quality soldiers and leaders who are trained to employ advanced IS technology. Organisations will be challenged to develop flexible task organised strategies using IS to adapt to the wide range of different conditions existing in the GIE. There will be some major challenges to both training and organisation, these are:

a. constantly advancing technology;

b. uneven distribution/fielding of equipment or capability; and

c. the search for and use of COTS products.

COMMUNICATIONS SUPPORT

19. Throughout all aspects of IO there is a paramount need for communications support to transport information, not only throughout the AO, but also, from a national or theatre level to an AO. This will involve numerous systems and all types of communications from strategic gateways to the forward most deployed elements of a force. Communication support requirements will be enormous, vary greatly and require maximum flexibility.

20. CIS must be adaptable and responsive to the commanders' requirements and should encompass the following characteristics:

a. digitize and compress multimedia tactical information using increased bandwidth, high efficiency transport systems;

b. encrypt and provide required levels of protection in all areas;

c. manage information networks with smart software and procedures that optimize capacity, throughout, and ensure dissemination and redundancy; and

d. display relevant common picture to commanders.

CAPABILITIES

21. Information requires end to end protected, seamless, high capacity, information transfer and processing capability in order for users to conduct effective operations throughout the battlefield. This capability will ultimately need to include multimedia operations, i.e., transportation of video, imagery, data, and voice. This will enable the commander to visualize the battle and battlefield from the current state to a successful end state. Some basic capabilities of the communication system will be:

a. to link the force to the MIE/GIE to achieve seamless connectivity across the field and garrison domain;

b. to provide high capacity hierarchical communications;

c. to broadcast broadband non-hierarchical information; and

d. to enable seamless split-base operations reaching back through strategic entry points to various platforms and information fusion centres.

FUTURE TECHNOLOGY

22. As it was stated previously one of the greatest challenges to IO is the pace and scope of technological change. Advances in information technology will allow commanders to form a more complete picture of the battlefield, generate the potential for faster, higher quality decisions, support more rapid manoeuvre in terms of time and space, and increase a unit's flexibility and agility. Of course technology is only a tool and no substitute for well trained leaders and effective tactical organisations. Some areas and indications of what could be possible in the near future are:

a. A tactical Internet capability which will enable information sharing and direct communications among and between virtually all users. This could enable a whole new level of non-hierarchical integration, co-ordination, and synchronisation that will coexist with the current vertical system.

b. The use of image compression and transmission technologies to allow transfer of images and video from various sensors and platforms enabling better understanding of the AO for planning, rehearsal, and execution of missions.

c. Finally, multimedia technology will enable three-dimensional presentation of imagery and graphics to enable commanders to visualize their AO far more effectively.

SECURITY

23. One of the greatest challenges and potential vulnerabilities is that of security. The increasing dependence on IS has created both increased capability but also increased vulnerability. Our computer systems and networks, which we depend on for virtually all aspects of administration, support, and operations are vulnerable to attack at any time. The Rand Corporation of the United States has stated that the anonymity of cyberspace has blurred the distinction between crime and warfare and between accident and attack. Gaining access to someone's computer or communications network can be accomplished by a wide range of methods and techniques, some of which are:

a. inserting malicious software through contractors;

b. tracking software maintenance changes and system operations activities; and

c. alternating access paths or sniffer devices that trap information about traffic and passwords.

24. These intrusions may be initiated at any time or any point in operation. Accordingly, security measures and procedures must actively, as well as passively preserve the confidentiality, integrity, and functionality of IS. Protection requirements include near real time measures that detect vulnerabilities, alterations, and intrusions, then react and counteract by restoring the IS. Some examples of these measures are:

a. procedures for quality assurance;

b. network and communication vulnerability assessment teams;

c. denial of unauthorised intrusion; and

d. hardening of programs.

25. The vast majority of intrusions result from human error. Training and Operational Security (OPSEC) compliance by system managers, operators, and users are the best measures to combat system compromises. In addition, system managers must be able to track down intruders.

26. In addition to tracking down intruders, system programs should be hardened against intruders attempts to gain information or damage information flow. No protection plan is perfect, and protection/restoration resources are finite. Plans and orders must specify the priority of protection effort.

COMMUNICATION AND INFORMATION SYSTEMS MANAGEMENT

27. Another critical area is that of the management of these systems. Because of the limitations of the communications environment (resources and technology) there will need to be a good IS management strategy that prioritises information. Commanders at all levels must carefully define their critical information requirements. It must be remembered that the purpose of automated IS is to achieve an information advantage by using and managing information for timely and accurate decision-making in all operations. The focus of the battle staff is to leverage available technology by employing IS that give the commander the desired information at the right time and place.

28. All information that the staff provides is predicated upon the commander's intent, concept of operations, and supporting commander's CCIRs. The CCIRs define the commander's information needs, thus focusing the staff and information support on the rapid acquisition, fusion, and analysis of information. The IS augment routing or periodic reports with specific requests for information.

29. Some of the activities and requirements include:

a. planning the Information Systems Network (to include information exchanges, database locations and replication);

b. planning communications connectivity;

c. planning network security;

d. allocating frequencies (to include effective spectrum management by G6 to support all aspects and types of IO);

e. controlling and monitoring the connection of systems;

f. reconfiguring the network as required;

g. maintaining and measuring network performance;

h. planning for degradation of the network; and

i. implementing continuity of operations plans as required.

CHAPTER 4
RELEVANT INFORMATION

In modern battle, the magnitude of available information challenges leaders at all levels. Ultimately, they must assimilate thousands of bits of information to visualize the battlefield, assess the situation, and direct the military action required to achieve victory.

US Army

SECTION 1
INTRODUCTION

1. This chapter sets the doctrinal foundation for the role of Relevant Information, which includes intelligence (see Figure 4-2-1). The chapter discusses the need for Relevant Information, the criteria to carefully assess such information, and the commander's decision-action cycle. It also includes information on the role of intelligence in framing Relevant Information about adversary forces.

SECTION 2
RELEVANT INFORMATION

2. Relevant Information is defined as information drawn from the Military Information Environment (MIE) that significantly impacts, contributes to, or relates to the execution of the operational mission at hand.

3. Relevant Information has a direct relationship with the MIE in two important ways:

a. first, the act of collecting, processing, or disseminating Relevant Information serves as the principal criterion a commander applies, to include an individual, organization, or system as part of the MIE; and

b. it is the product or medium drawn from or used by those same players that serves as the basis or currency of Information Operations (IO).

4. In the past the Army has tended to approach the collection and use of operational information from a specialized perspective. For

example, different sub-functions have collected and used information necessary to support their particular functions:

a. intelligence, focused upon information about the adversary and foreign nations;

b. operators, focused on situational information concerning friendly forces;

c. logisticians, focused on friendly force sustainment conditions and requirements; and

d. Public Affairs (PA) and Civil-Military Cooperation (CIMIC), focused on the interface between military and non-military sectors.

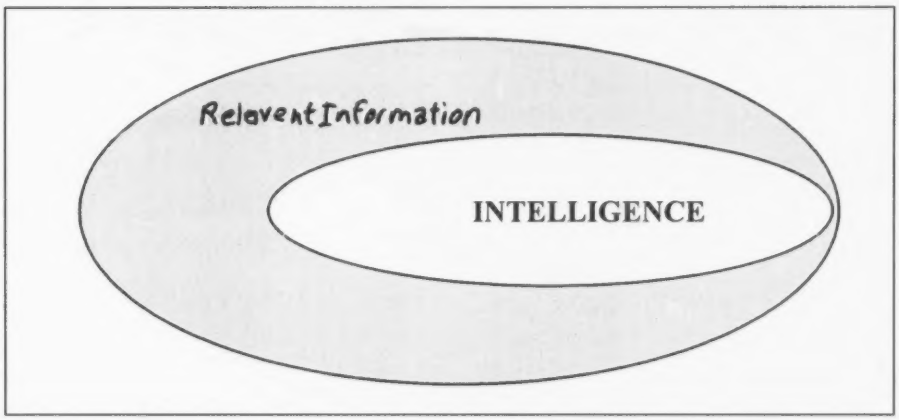

Figure 4-2-1: Relevant Information

5. Because of changes in the information and operational environments, we can now achieve new levels of efficiency and effectiveness in use of information by integrating and co-ordinating the collection, processing, and dissemination efforts. Efforts must focus on leveraging the potential operational contribution of information by efficiently collecting and sharing information across all elements.

SECTION 3
ASSESSMENT CRITERIA

6. Since sources of information are imperfect and susceptible to distortion and deception, commanders and planners must carefully assess

the quality of the information prior to its use. They can do so using the following six criteria:

a. **Accuracy**. Information that conveys the true situation.

b. **Relevance**. Information that applies to the mission, task, or situation at hand.

c. **Timeliness**. Information that is available in time to make decisions.

d. **Usability**. Information that is in common, easily understood formats and displays.

e. **Completeness**. All necessary information required by the decision maker.

f. **Precision**. Information that has the required level of detail.

7. As a first priority, information should be accurate and relevant. As a second priority, it should be both timely and in a usable form. Finally, information should be as complete and precise as possible. The following rule of thumb supports these relationships:

a. incomplete or imprecise information is better than none at all;

b. untimely or unusable information is the same as none at all; and

c. inaccurate or irrelevant information is worse than no information at all.

8. Commanders must have information to command. Information is the medium that allows the commander's decision-action cycle to function. Information gives direction to actions by the force, provides courses of action for protecting the force, and helps the force accomplish its operational mission. Relevant Information drawn from the MIE supports the creation of Situational Awareness (SA) that contributes directly to effective command during all stages of the decision-action cycle. The provision of an environment of profound SA helps the

commander ensure unity of effort toward mission accomplishment. Ultimately, effective command depends on the right person having the right information at the right time.

9. Commanders collect information, develop Battlefield Visualization, and plan for future operations at the same time as they conduct current operations. Meanwhile, senior and subordinate commanders gather information and work through decision-action cycles at their respective levels. Maintaining rapid decision-action cycles—and thus a rapid tempo of operations—requires that seniors and subordinates alike have an accurate, common picture of the area of operations (AO). From this common picture, a unit gains greater SA with which to exercise initiative during combat or other situations.

10. The commander operates within the Global Information Environment (GIE), adjusting his MIE to enhance his SA as necessary. Moreover, the commander uses his various means in the MIE to ensure that all elements of his force have a common, complete, and relevant multi-dimensional recognized common picture. This requires a sophisticated Communication Information System (CIS) that enhances the commander's ability to share, manage, and move information among organizations. The commander also uses his information capabilities to support Operations Other Than War (OOTW). The emphasis during OOTW missions shifts away from the combat to non-combat operations and starts to take on broader considerations contributing to efficient and effective operations. These operations often involve a variety of GIE players. For example, the G3 works closely with PA and CIMIC officers, among others, to determine critical information requirements pertaining to his AO.

SECTION 4
INTELLIGENCE

Intelligence is a term used to describe both the activities to acquire and process information and the product resulting from that process. Essentially, intelligence is information and knowledge about a belligerent obtained through observation, investigation, analysis, or understanding.

Source Unknown

11. Intelligence is the critical sub-element of the commander's Critical Information Requirements (CCIR) that focuses primarily upon foreign nations, environment and the adversary. In support of friendly operations, intelligence helps produce a common, current, and relevant picture of the AO, referred to as SA that reduces uncertainty and shortens the commander's decision-making process. In the future, intelligence activities will be conducted on the principle of split based operations enabling tactical commanders to draw upon or task strategic sensors and analytical capabilities. Intelligence support to operations executed at the strategic and national levels must be linked to support operations conducted at the operational and tactical levels. This effort requires a seamless intelligence collection process and supporting architecture, providing real-time, predictive intelligence products focused on CCIR, which will enable a commander's Battlefield Visualization (BV).

ROLE OF INTELLIGENCE

12. Intelligence, including Counter-Intelligence (CI), provides the commander with an accurate understanding of the threat situation as it relates to current and future operations. Intelligence personnel acquire, use, manage, and exploit information to produce an understanding of the adversary that is accurate and predictive. For common SA to be accurate and current, the intelligence effort is continuous. Intelligence collection includes all possible sources, from national-level covert operations through local open sources such as news media, commercial world contacts, academia, and persons.

13. In non-combat operations, Human Intelligence (HUMINT), open sources, and other government agencies provide timely information to

augment the unit's more traditional battle-focused intelligence-collection effort. The intelligence effort provides current, accurate threat and targeting data to weapon systems and intelligence sensors. Their effectiveness is dependent upon the rapid movement of data between collector, processor, decision maker, and shooter. Intelligence supports IO, focusing on Offensive and Defensive Information Operations.

INTELLIGENCE-ENABLING FUNCTIONS

14. The primary purpose of intelligence is to support operational decision-making based on an accurate understanding of the situation. The essence of intelligence is to collect, analyse, screen, and present information requested by the commander in the provision of current intelligence to support SA and with predictive materials to support BV. Intelligence-enabling functions focus on assessing friendly vulnerabilities, understanding the adversary, employing Intelligence Preparation of the Battlefield (IPB), and Battle Damage Assessment (BDA).

ASSESSING FRIENDLY VULNERABILITIES— COUNTER-INTELLIGENCE

15. The first critical step in protecting capabilities is to identify specific and potential threats by means of a CI estimate. Potential threats range from the adversary's direct overt and covert actions via its intelligence, surveillance, target acquisition and reconnaissance (ISTAR) array, to individuals and organizations seeking to exploit military CIS, to natural phenomena. They include a new family of global commercial imaging, cellular telephone, and positioning systems that jointly or separately provide a potential adversary with near real-time information on forces and movements.

16. The fluid and porous nature of the MIE makes it difficult to protect CIS from possible attacks. Therefore, intelligence provides the commander with the necessary information to conduct risk assessments and develop risk management options to protect vital Command and Control (C2) components and capabilities. The risk assessment is based on identification of such factors as specific threat capabilities, technical capabilities, doctrine, and past performance of the threat force. The risk assessment is not a finished document, but a continuous process that is constantly updated to reflect changes in the operating environment,

technology, and threat acquisitions. Because IO offers potential adversaries the chance to strike at the supporting infrastructure of the force—wherever it is located—the commander and his staff must be aware of threats to their CIS at the home station.

UNDERSTANDING THE ADVERSARY

17. The effectiveness of offensive operations, including IO, is predicated on a thorough understanding of an adversary, his C2 system, and his decision-making process. The deeper the understanding, coupled with tools and techniques to take advantage of such knowledge, the more effective will be the exploitation of the potential adversary. At all levels of operations, intelligence is an operational tool that identifies, assesses, and exploits the enemy's information and C2 systems. Data is required on what information the adversary collects, by what means, what reliability he places on various sources, and how that data is evaluated.

18. Intelligence personnel must be able to describe the enemy's decision-making process and how direction is sent to subordinates. Detailed intelligence is required on the social and cultural environments and the psychological makeup of the adversary's key leaders and decision-makers. How they interact and perceive one another are important aspects of the information necessary to develop effective Psychological Operations (PSYOPS) and deception operations. How subordinates execute decisions completes the picture. Having a detailed understanding of the adversary's use of information is necessary in order to determine where and how to effectively influence his actions.

> *Know the enemy and know yourself, and you will be victorious.*
>
> Sun Tzu (500 BC)

SECTION 5
EMPLOYING INTELLIGENCE—PREPARATION OF THE BATTLEFIELD

19. In applying IPB in the context of IO, the usual steps are followed. In step 1 of IPB, the battlefield environment is defined and the GIE as it pertains to the mission of the force is assessed. From this, it is possible in step 2 of IPB to describe the battlefield effects in order to define the MIE, with emphasis on:

a. the knowledge of the technical requirements on a wide array of CIS;

b. the knowledge of the political, social, and cultural influences at work in the MIE;

c. the ability to conduct highly technical processes to produce IO course-of-action templates; and

d. the identification of and in-depth understanding of the biographical, background of the adversary's key leaders, decision makers, communicators, and advisors.

20. Much of this information should be routinely collected and maintained in national-level databases and be readily available at the start of a mission. Even so, if an operation is ordered for a previously unforeseen AO, the intelligence officer must accomplish the steps of IPB beginning from first principles and raw information.

21. In the third step of IPB the intelligence staff construct a template of the adversary's force structure, doctrine, tactics, techniques and procedures. This template requires an estimate of the adversary's decision-making process. It is important to understand the information infrastructure of the adversary, which depicts how information flows within the unit, organization, and structure. This analysis includes human interface as a valid form of information distribution and is not limited to purely technological assessments. This aspect of IPB assists in developing an understanding of the leadership/personality profiles of the adversary's critical decision-makers. It addresses how they use information to make decisions, how they interact as organizations to make decisions, and how they execute those decisions. This step is linked directly to the ultimate goal of IO, which is to find ways to create a state of information superiority in the AO.

22. During this step, the intelligence officer analyses the decision-making template and the infrastructure template to determine adversary vulnerabilities. Vulnerability analysis occurs on two levels:

a. system vulnerabilities are identified and exploited to cause the desired effects on the decision process; and

b. the specific physical vulnerabilities of the system are determined.

23. Vulnerability analysis is then extended to include the collateral damage IO activities may cause on the operating environment. As an example, an option in attacking an adversary's C2 might be to destroy his electrical power infrastructure. However, the strategic cost (political or logistical) of destroying this capability might outweigh the tactical gains. One implication of the GIE is that actions and their consequences are examined across the MIE, as opposed to the battlefield alone.

24. Attainment of an understanding of the information infrastructure of the adversary, which depicts how information flows within the unit, organization, and structure is key to advancing to the fourth step of IPB, that of determining adversary Courses of Action (COA). Likewise, an understanding of how information from outside the adversary's unit, organization, or structure flows must also be developed for the commander's use. This includes understanding the local, regional, and global information environments. CIMIC teams operating in-country can greatly assist in this process.

25. In the fourth step of IPB the decision-making template and the infrastructure template are combined to form an adversary's IO COA template. The various COA open to the adversary can then be developed and analysed to determine the best way for us to use IO to influence, support, or accomplish the overall mission.

SECTION 6
ASSESSING BATTLE DAMAGE

26. Battle Damage Assessment (BDA), confirms or denies previous intelligence estimates and updates the IPB. The intelligence system continuously assesses the effectiveness on the adversary of all combat operations including IO. BDA allows commanders to adjust IO efforts to maximize effects. An important aspect of BDA is timely analysis to determine when an exploitable vulnerability is created in the adversary C2 structure. Compared to the way we look at conventional BDA reporting procedures, BDA in IO is not so apparent.

27. BDA in IO, is not always reported in terms of physical destruction of the target. The challenge of BDA is to be able to assess the effects of our efforts without the benefit of physical confirmation. The

effects may well be trends, activities, or patterns in future adversary actions. They could be as simple as an absence of activity on a C2 net, combined with an increase of traffic elsewhere, that is, reduced very high frequency/ultra high frequency (VHF/UHF) transmissions coupled with observations of increased courier traffic or heavy land line activity. BDA also examines the collateral damage Command and Control Warfare (C2W) actions may have caused to non-military systems and capabilities within a commander's MIE, for example the collapse of commercial telecommunications or a significant increase in security restrictions or official propaganda in the media.

CHAPTER 5
INTELLIGENCE, SURVEILLANCE, TARGET ACQUISITION AND RECONNAISSANCE IN LAND OPERATIONS

And Moses sent them to spy out the land of Canaan and said unto them, get you up this way Southward and go up into the mountain: And see the land, what it is; and the people that dwelleth therein, whether they be strong or weak, few or many.

Numbers 13:18-19

SECTION 1
INTRODUCTION

1. The aim of this chapter is to explain the Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) concept and how it fits in with the targeting process at formation level and the commander's Situational Awareness (SA). Previously the acronym RISTA (Reconnaissance, Intelligence, Surveillance, and Target Acquisition) was coined. In some quarters this suggested that reconnaissance was at the start of the process and was the most important component. The present manual has chosen to use ISTAR in order the emphasize the pre-eminence of the co-ordinating role of intelligence in the process, while not forgetting that the sole purpose of ISTAR is to support the commander in his decision-making process. It is not an end unto itself.

2. Most views of future operations accept that the information age is, and will be, characterized by the proliferation of information systems and the rapid passage of information. Collection, control and exploitation of this information, through all means, are prerequisites for successful military operations. This applies across the whole continuum of operations from non combat to combat operations. This chapter however retains its focus at the combat operations end of the continuum.

3. Canadian military doctrine is manoeuvrist in its approach to operations. The essence of the manoeuvrist approach to operations is to be able to shatter the enemy's cohesion and destroy his will to fight without necessarily engaging in large scale action. In order to achieve this, it is necessary to identify the enemy's key weaknesses and exploit them by concentrating force or inducing a belief in the enemy that decisive force is about to be used. A comprehensive ISTAR capability is

essential if a manoeuvrist approach is to be successful. It allows commanders to work within the enemy's decision-action cycle and successfully fight high tempo, multi-action battles without suffering unnecessary losses to friendly forces.

4. The differing requirements of each operation will dictate how ISTAR assets are organized and employed. Each operation will have its own unique set of information requirements and these requirements are met by tasking a wide range of ISTAR assets.

SECTION 2
THE ISTAR CONCEPT

5. ISTAR links surveillance, target acquisition, and reconnaissance to improve a commander's SA and to cue manoeuvre and offensive strike assets.

6. An ISTAR system can be defined as a structure within which information collected through systematic observation is integrated with information collected from specific missions and processed in order to meet the commander's intelligence requirements. It also permits the detection, identification and location of targets in sufficient detail and in a timely enough manner to allow their successful engagement by weapon systems. It is a system, which is comprised of the following components:

a. sensors, which act as collection assets;

b. processors, which act as an information collection and analysis system;

c. an information and sensor management system; and

d. an effective system linking ISTAR assets and the commander.

7. The basis of the ISTAR system is that all ISTAR assets at a particular level of command are controlled and managed centrally by a single ISTAR co-ordinator. This function is carried out in a formation Intelligence Collection and Analysis Centre (ICAC) or by the intelligence staff at unit level. Intelligence provide commanders and staffs with timely and accurate intelligence on the enemy, weather and terrain together with

Relevant Information. The ISTAR concept generates the necessary synergy by:

a. providing the necessary mix of collection assets and information system technologies at each level of command;

b. using appropriate technologies to integrate and co-ordinate the collection aspect of ISTAR; and

c. improving the sharing and dissemination of information/intelligence.

8. The ISTAR system, when well-conceived and properly executed, provides the best mixture of personnel, equipment, and command and control procedures to:

a. reconnoitre specific targets or areas;

b. maintain a continuous and systematic, 24 hour-a-day, all-weather watch, of air, surface and electromagnetic spectrum, over an AO; and

c. process gathered information into all-source intelligence products.

9. Information requirements, resources, time available and the threat determine the mixture of ISTAR resources employed.

SECTION 3
THE PRINCIPLES OF ISTAR

10. The principles of ISTAR can be summarized as follows:

a. **Centralized Co-ordination**. ISTAR must be co-ordinated at the highest level of command without sacrificing the principle of mission command. This ensures the most effective and efficient use of resources.

b. **Responsiveness**. The system must be able to react quickly to the commander's information and

intelligence requirements and be rapidly able to exploit targeting information.

c. **Continuous Coverage**. Surveillance, target acquisition and reconnaissance must be able to provide coverage 24/7 in all weather.

d. **Robustness**. ISTAR assets must provide a robust mix of overlapping systems in terms of technology, range and performance in order to cope with enemy action as well as changing meteorological and light conditions and to defeat adversary deception plans.

e. **Timeliness**. Information and intelligence must be provided to the commander in a timely fashion to allow him to work within the enemy's decision-action cycle.

f. **Accuracy**. The ISTAR product must be accurate and relevant to the operation it is supporting.

g. **Passage of Information**. Within an ISTAR system it must be possible to pass information between appropriate commanders and staffs without overloading them with irrelevant data.

SECTION 4
THE ACTIVITIES OF ISTAR

11. The following definitions are essential for understanding ISTAR:

a. **Intelligence**. The product resulting from processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. (AAP-6(U), *NATO Glossary of Terms and Definitions*)

b. **Battlefield Surveillance**. Systematic observation of the battle area for the purpose of providing timely information and combat intelligence. (AAP-6 (U))

c. **Target Acquisition**. The detection, identification and location of a target in sufficient detail to permit the effective employment of weapons. (AAP-6(U))

d. **Reconnaissance**. A mission undertaken to obtain by visual observation or other detection methods, information about activities and resources of an enemy or potential enemy, or to secure data concerning the meteorological, hydrographic or geographic characteristics of a particular area. (AAP-6(U))

12. The component parts of ISTAR are closely linked and often overlap. Together they involve:

a. **Area Surveillance**. Continual area surveillance provides for the collection of general information on an enemy or potential enemy. It may be used to:

(1) provide basic information on deployments, activity levels, capabilities and overall intentions;

(2) cue reconnaissance and target acquisition resources to investigate specific activities or to obtain more detailed data/information on a particular observation;

(3) provide limited security to friendly forces through early warning of enemy activity within gaps, on exposed flanks or in rear areas; and

(4) assist in initial target recognition and identification.

b. **Deep Reconnaissance**. Reconnaissance in depth aims to provide detailed information in areas beyond the range of direct fire weapons. It can be initiated as the result of area surveillance or by intelligence deductions. It may involve:

(1) the identification of known or suspected enemy forces including composition and activities;

(2) the acquisition of targets for air, aviation and indirect weapon systems; and

(3) the location and tracking of specifically targeted enemy units, elements or activities.

c. **Close Reconnaissance**. Close reconnaissance satisfies the requirements for both combat information and target acquisition essential for troops in or near contact with the enemy.

d. **Target Acquisition**. Target acquisition is the process of providing detailed information and locating forces with sufficient accuracy to enable those elements to be selected as targets. It includes:

(1) **Target Acquisition for Direct Fire Weapons**. Normally associated with a specific weapon, such a system provides essential combat information on an enemy that has already been detected, located and may now be engaged.

(2) **Target Acquisition for Indirect Fire Weapons**. Normally a data/information collection means operating beyond the line of sight of friendly forces and providing information to one or more indirect weapons systems.

SECTION 5
SOURCES AND AGENCIES

13. **General**. The difference between a source and an agency is that the former provides information and the latter intelligence. Different sources use a variety of techniques and disciplines to acquire their information. The components of intelligence, Signal Intelligence (SIGINT), Human Intelligence (HUMINT), Image Intelligence (IMINT), Open Source Intelligence (OSINT) and Acoustic Intelligence (ACCOUSINT) are explained in B-GL-351-001/FP-001, *Combat*

Intelligence. Intelligence agencies normally require information input from a number of sources (and sometimes other agencies) before making a considered assessment.

14. **Sources**. These will include:

a. screen, guard and covering troops;

b. stay behind parties;

c. forward units, patrols and observers;

d. specialist reconnaissance and locating troops;

e. aircraft, helicopters and unmanned aerial vehicles (UAVs);

f. electronic warfare (EW) assets; and

g. prisoners and refugees.

15. **Agencies**. These include:

a. intelligence staff (G2, artillery, engineer or unit) at battle group, brigade, division, and corps HQs;

b. G3, air and EW staffs at brigade, division and corps HQs;

c. long range reconnaissance patrol (LRRP) organization;

d. SIGINT/EW Co-ordination Cell at corps; and

e. interrogation organization.

16. At corps, division and brigade group level agencies are formed into an ICAC to co-ordinate the processing and gathering of intelligence.

SECTION 6
ISTAR PLANNING AND EXECUTION

17. **Planning**. The process leading to the ISTAR plan goes through the following steps:

a. carry out mission analysis;

b. establish Priority Intelligence Requirements (PIR);

c. identify Named Areas of Interest (NAI) and Target Areas of Interest (TAI); and

d. develop the collection plan.

18. **Execution**. The basis for the effective employment of ISTAR assets of any formation is a comprehensive collection plan. Prior to issuing any tasking a commander and his staff must:

a. analyze and validate the requirement to conduct the ISTAR activity under consideration;

b. determine the priority of the requirement;

c. review all ISTAR assets available and select the most appropriate; and

d. request the information and intelligence required, with the appropriate degree of priority, from superior and neighbouring formations for areas beyond their Area of Operations (AO).

19. Once the requirement for an ISTAR tasking has been validated and approved, one or more collection systems must be tasked. For collection from outside the Area of Intelligence Responsibility (AIR) of the formation and from agencies not under command, a request must be made through the superior headquarters. Agencies may include:

a. **Ground Systems**. Passive, active or hybrid (passive until triggered);

b. **Air Systems**. Passive or active;

c. **Satellite/Space Systems**; and

d. **Information Systems**.

20. Rapid part processing, initial assessments and full intelligence processing have, with advances in technology, become integral parts of any ISTAR activity. The inherent processing capabilities of certain ISTAR assets are such that valuable information can be derived from the system as it conducts its mission. Appropriate provision should, therefore, be made for the timely dissemination of both the unprocessed and combat information obtained and also the final processed intelligence product.

21. Once an ISTAR task has been completed the results achieved must be assessed against the original requirement as stated in the collection plan. A decision on whether the requirement has been met or is no longer valid must also be made. The plan is then updated and further staff action is initiated if appropriate. Notwithstanding the above, the intelligence cycle is a dynamic and continual process. The intelligence requirement and relative priorities will be constantly changing and need to be reviewed regularly.

SECTION 7
THE TARGETING PROCESS

22. **Introduction**. Targeting is defined as "*the process of selecting targets and matching the appropriate response to them, taking account of operational requirements and capabilities.*" It fuses ISTAR with weapon systems such as air, aviation, indirect fire and Offensive Intelligence Operations (Off IO), ensuring that the capabilities of each are used to maximum effect. Good targeting is fundamental to speed of reaction, and is thus a G3 responsibility co-ordinated as part of the overall Concept of Operations. Clearly however there is significant G2 input.

23. **Level of Command**. Effective targeting requires time, staff effort, and access to the full range of ISTAR and weapon systems. It is, therefore, primarily implemented at divisional level and above and optimised for engagement of depth targets. The principles can however be applied at brigade level and below with suitable modification.

24. **Concept**. Targeting is an integral part of the planning process, requiring co-ordinated effort by several staff branches. It begins with receipt of the mission and is thereafter inextricably linked to the Operational Planning Process (OPP) and Intelligence Preparation of the Battlefield (IPB) as the overall plan is developed. There are four phases to the targeting cycle:

a. **Decide**. As many decisions as possible are taken during the planning process so that targeting action can take place immediately when an opportunity arises, without further reference to the commander. Priorities need to be stated for:

(1) the tasking of target acquisition assets;

(2) information processing;

(3) use of attack assets; and

(4) the requirement for Battle Damage Assessment (BDA).

b. **Detect**. Though some target acquisition assets may provide actual targets, other assets must have their information product assessed to detect targets. Once identified, targets must be tracked until they can be engaged. Assets used for this purpose will be unavailable to detect new targets.

c. **Deliver**. At this stage targets are attacked in accordance with the commander's priorities laid down during the decide phase.

d. **Assess**. The results of an attack must be assessed to ensure the intended effect has been achieved.

25. Targeting facilitates the co-ordination of ISTAR and strike assets such as air, aviation, indirect fire and Off IO ensuring that they are properly integrated and that the most appropriate weapon system is used to attack each target. Further information on this subject can be found in B-GL-300-007/FP-001, *Land Force Firepower*.

CHAPTER 6
OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS

Command is the most important activity in war.[4]

SECTION 1
INTRODUCTION

1. The aim of this chapter is to explain the offensive and defensive components of Information Operations (IO). IO are nothing really new. What is new is the increased importance placed on command and on shaping beliefs of the persons in the Area of Operations (AO). Without effective Command and Control (C2) a military force will fail despite having a superiority in weapons equipment and manpower.

2. The same is true about the cohesion of people. An important sub-set of Offensive and Defensive IO (Off IO and Def IO) was termed Command and Control Warfare (C2W). C2W was aimed primarily at C2 systems and therefore was too restrictive when compared to the real world application of IO as experienced during operations. The definition of Off IO and Def IO is broadened to deal with shaping the beliefs of people in the AO and to include the activities of Counter-Intelligence (CI), Counter-Psychological Operations (counter-PSYOPS), Computer network attack (CNA) and Special Information Operations (SIO).

3. Off IO and Def IO are nothing more than a co-ordinated approach to attacking an adversary's ability to command, including shaping the beliefs of the hostile and neutral people while ensuring that our command remains effective and that our population is protected. As integral components of IO, Off IO and Def IO support the Army's manoeuvrist approach to operations.

4. There has been a significant increase in the ways and means of attacking an adversary's people, command and command support systems. This has increased the vulnerabilities. To be effective, IO need to be fully integrated into the commander's concept of operations and co-ordinated.

---

[4] B-GL-300-003/FP-000, *Command*

5. C2W was defined as "*The integrated use of all military capabilities including operations security (OPSEC), deception, psychological operations (PSYOPS), electronic warfare (EW) and physical destruction, supported by all source intelligence and Communication Information Systems (CIS), to deny information to, influence, degrade, or destroy an adversary's C2 capabilities while protecting friendly C2 capabilities against similar actions.*"[5]

6. Off IO and Def IO information operations directly support the goal of achieving information superiority and winning any conflict including Operations Other Than War (OOTW), quickly, decisively, and with minimum casualties. This combination of both offensive and defensive aspects into an integrated capability provides expanded opportunities for synergy in warfare. IO allows the Army and individual commanders to accomplish missions with fewer risks, in shorter time frames, and with fewer resources.

ROLE OF OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS

7. Off IO and Def IO are applicable to all phases of operations, including those before, during, and after actual hostilities. Even in OOTW, they offer the military commander lethal and non-lethal means to achieve the assigned mission while deterring war and/or promoting peace. The offensive aspect of IO can slow the adversary's operational tempo, disrupt his plans and ability to focus combat power, and influence his estimate of the situation. The defensive aspect of IO minimizes friendly personnel and C2 system vulnerabilities and mutual interference. Off IO and Def IO apply throughout the spectrum of conflict. Def IO will not normally be restricted in peace time, however, Off IO will be controlled through Rules of Engagement (ROE).

---

[5] MC 348, *NATO Command and Control Warfare Policy*

SECTION 2
ELEMENTS

8. The foundation for IO is a robust CIS, coupled with seamless, national-to-tactical, Relevant Information and intelligence support. The elements of Off IO and Def IO are:

a. OPSEC;

b. CI;

c. military deception;

d. PSYOPS;

e. counter-PSYOPS;

f. electronic warfare (EW);

g. CNA;

h. SIO; and

i. physical destruction.

9. These elements contribute to the protection of the force and mission accomplishment in various ways, depending on the situation. The integrated employment of these elements leads to synergy on the battlefield and results in the most effective execution of Off IO and/or Def IO focusing attacks on the adversary, its commander and his ability to command and control forces while simultaneously protecting friendly C2 and forces.

RELEVANT INFORMATION

10. Successful application of Off IO and Def IO in operations is critically dependent on accurate, relevant and timely information and intelligence. The adversary's commanders and their support systems must be determined in order to successfully execute Off IO. Equally important, today's commanders must understand the vulnerabilities of our own systems and take the necessary actions to protect ourselves from attack.

The increased number of Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) assets available to a commander and the co-ordination of their activities and products can no longer be stove piped as in the past.

COMMUNICATION INFORMATION SYSTEMS

11. CIS are critical. They are the pipelines that allow the information activities (acquire, deny, use and protect) to be carried out. CIS are therefore a major target for our Off IO effort. The reliance that the Army places on CIS now and in the future has created significant vulnerabilities for commanders and command support systems. Knowing our own vulnerabilities is the key to protection.

OPERATIONS SECURITY

12. Operations security is defined as "*The process which gives a military operation or exercise appropriate security, using passive or active means, to deny the enemy knowledge of the dispositions, capabilities and intentions of friendly forces.*"[6]

13. OPSEC gives the commander the capability to identify those actions that can be observed by adversary intelligence systems. It can provide an awareness of the friendly indicators that adversary intelligence systems might obtain. Such an awareness could be interpreted or pieced together to derive critical information regarding friendly force dispositions, intent, and/or courses of action that must be protected. The goal of OPSEC is to identify, select, and execute measures that eliminate, or reduce to an acceptable level, indications and other sources of information that may be exploited by an adversary.

14. OPSEC planning faces multiple challenges from the new family of global commercial capabilities, to include imaging, positioning, and cellular systems that offer potential adversaries access to an unprecedented level of information against friendly forces. The inevitable presence of the news media during military operations complicates

---

[6] NATO AAP 6 (U)

OPSEC. The capability of the media to transmit real-time information to a world wide audience could be a lucrative source of information to an adversary. OPSEC planners, working closely with Public Affairs (PA) personnel, must develop the Essential Elements of Friendly Information (EEFI) used to preclude inadvertent public disclosure of critical or sensitive information.

15. Many different measures impact OPSEC. These include CI, Information Security (INFOSEC), Transmission Security (TRANSEC), Communications Security (COMSEC), and Signal Security (SIGSEC). As more and more of the force is digitized, INFOSEC takes on an ever-growing importance.

COUNTER-INTELLIGENCE

16. CI consists of those intelligence activities related to assessing own forces vulnerabilities to an adversary's intelligence capabilities, such as an ISTAR array and in neutralizing those vulnerabilities. CI is at once reactive to Security Intelligence (SECINT) and combat intelligence and supports OPSEC. See B-GL-352-001/FP 001, *Combat Intelligence,* for more information.

MILITARY DECEPTION

17. Deception is defined as "*those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests.*"[7] Military deception is the primary means to influence the adversary commander's decisions through distortion, concealment, and/or falsification of friendly intentions, status, dispositions, capabilities, courses of action, and strengths. The goal of deception is to cause the opposing military commander to act in a manner that serves the friendly commander's objectives.

HISTORICAL PERSPECTIVE

Tactical deception had significant positive impacts on the success

---

[7] NATO AAP 6 (U)

of Operation OVERLORD, and, thus the retaking of the European continent in World War II. Deception worked hand in hand with OPSEC to keep the organization and location of the real OVERLORD cantonments, training sites, dumps, movements, and embarkations carefully hidden. Unbelievable effort was put into creating mock airfields and ports, phoney ships, boats, planes, tanks, vehicles, and troop movements, both real and staged. A new era of deception was introduced–the electronic one. German coastal defence radars were destroyed in a calculated pattern. Deception planners purposely left some intact in the Calais region. The night the invasion was launched, the Allies began massively jamming German radars with chaff. But, they purposely did not completely cover their targets. German radar operators could "see" between Allied jamming curtains. And, what they saw was a ghost fleet of small ships towing barges and blimps headed for Calais at eight knots–or the speed of an amphibious fleet. Powerful electronic emitters received the pulse of the German radar and sent it strongly back to the German receivers. For each repetition of this deception it looked to the German operators like a 20,000-ton ship was out there. The small ships also had the recorded sounds of the amphibious assault at Salerno to play over speakers from 10 miles out. German troops ashore could hear the Allies "getting into their landing craft" for the run into the beach. This information threw German intelligence into chaos for several precious hours and played a major role in delaying German counteractions to the actual invasion, taking place at Normandy.

PSYCHOLOGICAL OPERATIONS

18. Psychological Operations are defined as "*planned psychological activities in peace, crisis and war directed to enemy and neutral audiences in order to influence attitudes and behaviour affecting the achievement of political and military objectives.*"[8]

19. PSYOPS are conducted to convey selected information and indicators to foreign audiences in order to influence their emotions,

---

[8] NATO AJP 1

motives, objective reasoning, and, ultimately, the behaviour of foreign governments, organizations, groups, and individuals. The purpose of PSYOPS is to induce or reinforce foreign attitudes and behaviour favourable to the originator's objectives.

20. PSYOPS are based on the projection of the truth and of credible messages. PSYOPS are an essential tool in both Off IO and Def IO. PSYOPS elements must co-ordinate with other C2W elements and PA strategists to maximize the advantage of IO. As an example, the Army has shown considerable strength in applying PSYOPS to military operations in Haiti.

21. PSYOPS main objective in Def IO is to minimize the effects of an adversary's hostile propaganda and misinformation campaign against the Canadian Forces. Discrediting adversary propaganda or misinformation against the operations of coalition forces is critical to maintaining favourable public opinion.

COUNTER-PSYOPS

22. The aim of Counter-PSYOPS is to shield an audience from hostile messages and lessen their impact. In this context, PSYOPS aim to counter information, beliefs, attitudes and behaviour detrimental to the objectives of a Canadian Forces operation. Any misinformation or disinformation propagated will be exploited by political extremists, paramilitary and military groups to gain public support for their objectives.

ELECTRONIC WARFARE

23. Electronic Warfare is defined as "*military action involving the use of electromagnetic (EM) energy, including direct energy (DE), to exploit and dominate the EM spectrum or to attack an enemy. It encompasses the interception and identification of EM emissions, the employment of EM energy to reduce or prevent hostile use of the EM spectrum and actions to ensure its effective use by friendly forces. The three divisions of EW are: electronic countermeasures (ECM); electronic*

protective measures (EPM); and electronic warfare support measures (ESM)."[9]

24. ECM is the attack component of EW. ECM is defined as "*that division of EW involving actions taken to prevent or reduce an enemy's effective use of the EM spectrum, through the use of EM energy.*" There are three sub-divisions of ECM: electronic jamming, electronic deception and electronic neutralization.[10] ECM can attack the adversary anywhere from his tactical formations, back to his national infrastructure. (The US Army uses the term Electronic Attack (EA)).

25. EPM is the protection of the friendly use of the EM spectrum. EPM is defined as "*that division of EW involving actions taken to ensure friendly effective use of the EM despite the enemy's use of EM energy.*"[11] EPM covers the gamut of personnel, equipment, and facilities. EPM is part of survivability. As an example, self and area protection systems can interfere with the adversary's target acquisition and engagement systems to prevent destruction of friendly systems and forces. (The US Army uses the term Electronic Protection (EP)).

26. ESM is defined as "*that division of EW involving actions taken to search for, intercept and identify EM emissions and locate their sources for the purpose of immediate threat recognition. It provides a source of information required for immediate decisions involving ECM, EPM and other tactical actions.*"[12]

27. ESM conflict-related information involves actions tasked by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy to detect immediate threats. ESM is the embodiment of combat information and capitalizes on the timeliness of sensor-to-shooter systems. ESM can best be described as electronic

---

[9] ATP 51(A), *NATO Electronic Warfare in the Land Battle*

[10] ATP 51(A)

[11] ATP 51(A)

[12] ATP 51(A)

reconnaissance and surveillance. ESM can be conducted by single detachments in support of units or sub-units or complete systems in support of formations.

28. EW is no longer just a specialist issue for specialist units. EW of the future will tend toward platform protection of high value targets in the same way the Navy and Air Force protect ships and aircraft. EW is a significant ISTAR capability which can be used alone but is considerably more effective if used with other ISTAR capabilities, such as Unmanned Aerial Vehicles (UAVs), in a coordinated system.

COMPUTER NETWORK ATTACK

29. Computer Network Attack is defined as "*Operations to disrupt, deny, degrade or destroy information resident in information systems, or the information systems themselves.*"[13] CNA and ECM are both elements of Off IO, and ECM could be used as a means to conduct CNA.

SPECIAL INFORMATION OPERATIONS

30. Special Information Operations are defined as "*IO of a sensitive nature which, owing to its potential effect or impact, security requirements, or risk to the national security of Canada, requires a special review and approval process.*"[14]

PHYSICAL DESTRUCTION

31. Physical destruction is defined as "*the application of combat power to destroy or neutralize enemy forces and installations. It includes direct and indirect fires from ground, sea, and air forces. Also included are direct actions by special operations forces.*"

---

[13] Canadian Forces Information Operations Policy 4th draft

[14] B-GG-005-004/AF-032 *Canadian Forces Information Operations Doctrine*

32. The destruction of a hostile C2 target means that adversary C2 capabilities are degraded for a period of time or, if necessary, permanently shut down. Physical destruction is used only after a full, comparative assessment, strategic through tactical perspectives, of the trade-offs between preserving the target versus its destruction.

HISTORICAL PERSPECTIVE

On April 14, 1943, US intelligence experts intercepted and decoded a message revealing that Admiral Isoroku Yamamoto, Commander-in-Chief of Japan's Navy, would be flying to Bougainville in four days. When analysis determined that Bougainville lay just within the extended range of US P-38 fighters at Henderson Field on Guadalcanal, Allied planners recognized the opportunity to strike at the heart of Japanese command and control and strategic planning in the Pacific. In less than 48 hours, Admiral Chester W. Nimitz's forces planned and coordinated an operation to shoot down Yamamoto's plane and obtained approval from Secretary of the Navy Frank Knox and President Roosevelt. Yamamoto was known to be invariably punctual, and American planners were confident that his plane would appear over Bougainville on schedule–9:39 am, April 18. At that moment, 16 carefully positioned P-38s from Henderson Field spotted the two Japanese Betty bombers of Yamamoto's party and attacked. Both aircraft were quickly sent plummeting to the ground, completing a classic information operation that took less than four days from start to finish and rendered irreparable damage to Japanese command and control. The Japanese would feel the impact of this single mission throughout the remainder of the war.

SECTION 3
OFFENSIVE INFORMATION OPERATIONS

33. **Off IO**. Off IO are defined as "*the synchronized execution of actions taken to accomplish established objectives that prevent effective C2 of adversarial forces by denying information to, by influencing, by degrading, by destroying the adversary's C2 system or by influencing beliefs of hostile persons.*"

34. **Off IO Principles**. The three principles of Off IO are to:

a. Plan based on the unit's mission, commander's intent, and concept of operations.

b. Synchronize with and support the commander's plan.

c. Take and hold the initiative by degrading the adversary's CIS and forcing him to be reactive. Reactive means that Off IO slows the adversary's tempo, disrupts his planning and decision cycles, disrupts its commander's ability to generate combat power, and degrades its commander's means for executing mission orders and controlling subordinate unit operations.

35. **Off IO Effects**. In general terms, Off IO have four effects that focus on the adversary's C2 infrastructure and information flow to produce a lower quality and slower decision-making cycle. These are:

a. First, the adversary is denied information by disrupting his observation, degrading his orientation and decision formulation, and degrading information collection. Information collection can be degraded by destroying collection means, by influencing the information the adversary acquires, or by causing him not to collect at all.

b. Second, the adversary commander is influenced by manipulating perception and causing disorientation of his decision cycle.

c. Third, adversary IO are degraded by selectively disrupting Command, Control Communications, Computer and Intelligence (C4I) systems.

d. Fourth, adversary information capabilities can be neutralized or destroyed by physical destruction of nodes and links. Destruction operations are most effective when timed to occur just before he needs a certain C2 function or when focused on a target that is resource-intensive and hard to reconstitute.

36. Off IO can also have a significant effect on the beliefs and cohesion of the enemy troops and population. The mutual support between all elements of Off IO and Def IO is detailed in Annex A.

HISTORICAL PERSPECTIVE

Heraclitus of Ephesus in sixth century BC noted that "if you do not expect the unexpected, you will not find it." During the German invasion of the Soviet Union in June 1941, the Germans recognized, but the Russians did not, exploitable deficiencies in the existing Soviet C2 system. Employing the tools of C2W in an interrelated fashion, the Germans were able to effectively disrupt, exploit, and destroy the Soviet C2 system. Using weapons specifically built for C2W, the Germans attacked elements of the Soviet system by air, artillery, and sabotage. The results of these attacks were startling. Due to cross-border German sabotage efforts, many of the Soviet units "did not receive the war alert order when it was issued [from Moscow] on the night of 20-21 June 1941." By 24 June, large gaps had already been torn in the Soviet communications network, thus forcing commanders to rely on easily exploitable, unprotected, radio networks. This, in turn, led to the successful targeting of exposed command posts and associated units throughout the theater. These attacks, because of their effectiveness, led Soviet commanders to prohibit the use of radios because they might give positions away. Using C2W, the Germans had effectively shut down the Soviet C2 system, creating an operational environment that quickly led to a general collapse of the entire eastern front.

SECTION 4
DEFENSIVE INFORMATION OPERATIONS

37. **Def IO.** Def IO are defined as "*the maintenance of effective C2 of ones own forces by turning to friendly advantage or negating adversary efforts to deny information, to influence, to degrade, or to destroy the friendly C2 system as well as the protection of own troops, friendly and neutral personnel against the effects of enemy Off IO.*"

38. Def IO can be proactive or reactive. Proactive Def IO use the elements of Off IO and Def IO to reduce the adversary's ability to conduct Off IO. Reactive Def IO reduce friendly vulnerabilities to adversary Off

IO by employing adequate physical, electronic, and intelligence protection.

39. **Def IO Principles**. The Def IO process can best be understood by reverse engineering our Off IO process. Commanders ask how the adversary can employ destruction, EW, CNA, military deception, OPSEC, SIO, and PSYOPS to disrupt our C2 systems, decision-making process and the beliefs of our people. Having war-gamed the adversary's Off IO courses of action, the commander can develop a comprehensive Def IO posture, synchronized with the main effort and Off IO. The commander is guided by the six principles of Def IO. These principles are:

a. To gain C2 superiority. This principle includes functions such as the unimpeded friendly processing of information, accurate development of courses of action, valid decision-making, and efficient communications to and from subordinates.

b. To stay inside the adversary's decision cycle. This is done by denying, influencing, degrading, and/or destroying the adversary's C2 personnel, equipment, and systems.

c. To reduce the adversary's ability to conduct Off IO.

d. To reduce friendly C2 vulnerabilities using Def IO measures. As an example, countering the effects of adversary propaganda or misinformation through PSYOPS and PA.

e. To reduce friendly interference in our C2 systems throughout the EM spectrum(de-conflict and co-ordinate).

f. Ensure the troops and the population are well informed of the situation within the bound of OPSEC.

HISTORICAL PERSPECTIVE

The history of the Information Age is being made now. In 1988 we saw the first well-publicized case of a computer virus. This insidious, self-replicating virus known as the Internet Worm penetrated the computer system at the University of California at Berkeley, corrupting thousands of computers on the Internet. A computer emergency response team (CERT) had been created at Carnegie Mellon University. In 1993 they had their first large event as they put out a warning to network administrators that a band of intruders had stolen tens of thousands of Internet passwords.

When CERT began in the late 1980s, they processed less than 50 events per year. Now they are in the thousands per year. The military is a target of this attack. Recent stories have told of a 16 year old who compromised the security of more than 30 military systems and more than 100 other systems before he was caught after a 26-day international electronic manhunt. This experience hints at the impact a professional, well-financed effort could have against computer nets. The lesson this evolving history is showing us vividly today is that the information highway is creating a great vulnerability to the Canadian Forces. We are all familiar with the security of transmitting information over a radio or telephone. But there is an even greater weak spot now in computers, databases, software (such as decision-making aids and tools), servers, routers, and switches. This vulnerability exists today and is growing in geometric proportions.

40. **Def IO Effects**. The effects of Def IO mirror those of Off IO. We can deny information the adversary needs to take effective action. We can influence the adversary not to take action, to take the wrong action, or to take action at the wrong time. We can degrade and destroy his capabilities to perform Off IO against friendly forces. Counter-PSYOPS and PA supports Def IO. PSYOPS can drive a wedge between the adversary leadership and its populace to undermine the adversary leadership's confidence and effectiveness. The commander's Internal Information Program, publicized by the Public Affairs Officer (PAO), can be extremely beneficial in countering adversary propaganda in Canada and among the deployed forces. PA specialists, working with PSYOPS and intelligence personnel, can also develop information products that commanders can use to help protect soldiers against the effects of adversary misinformation or disinformation.

SECTION 5
CO-ORDINATION

41. B-GL-300-003/FP-000, *Command,* discussed the importance placed on command. IO is a command driven function aimed directly at the adversary and its commander while protecting ourselves. Although all commanders may not have all the capabilities within their units to conduct all aspects of Off IO and Def IO, it is imperative that all commanders recognize which activities they can conduct and understand their portion of a larger plan.

42. IO is a COS/G3 responsibility for planning and co-ordination on behalf of the commander. IT IS NOT A SPECIALIST ACTIVITY. At the formation level an IO officer may be designated to assist the COS/G3 in planning and co-ordinating the formation IO effort. Specialist advisors will be needed based on the IO capabilities of the formation. An IO annex should be a component of all operations orders. IO co-ordination and planning activities will be conducted in accordance with B-GL-331-001/FP-001, *Command Support Doctrine.*

CHAPTER 7
PUBLIC AFFAIRS

A hostile press is more to be feared than 5 army corps.

Napoleon

SECTION 1
INTRODUCTION

1. The modern battlefield has changed dramatically and so has the ability of the news media to report from the battlefield. Technological advances ensure that future operations will unfold on a global stage before a world-wide audience, with tactical actions and the hardships of soldiers and civilians alike having an increasing impact on strategic decision-making. Real-time visual images of operations, both positive and negative, will continue to influence public understanding and support. For example, in 1992, US soldiers landed under the glare of media camera spotlights on the beaches of Mogadishu and the images were transmitted in real-time to audiences around the world. In 1996, Canadian soldiers landing at the Kigali airport in Rwanda for Operation Assurance were met with a similar media barrage and their actions were broadcast to a largely European audience in near real-time

2. In essence, the presence of the news media has become a battlefield reality. This reality must be considered when planning military operations. News media capabilities and requirements must be understood and accounted for by mission planners. Failure in this regard will not prevent the media from covering our operations, but it will ensure that they go to alternate sources for their information and perhaps create a situation that endangers the success of the operation they are trying to cover.

3. Commanders with the information and capability to shape all dimensions of the Area of Operations (AO) can organize and control forces with the speed and timing necessary to win. However, the commander's information needs are not found in a single source, but in a combination of many systems and functions, including the news media.

SECTION 2
INFORMATION ENVIRONMENT

4. The Global Information Environment (GIE) contains those information processes and systems that are beyond the **direct influence** of the military, but which may directly impact on the success or failure of military operations. The media, international organizations and even individuals are players in the GIE.

5. All Army operations can be influenced through planned or inadvertent messages communicated via the GIE. News of military operations can be broadcast in real-time, or near real-time, to our troops, the Canadian public, our allies, adversaries and indeed, any belligerent force involved in an operation. Unofficial public analysis, critiques and commentaries can affect on-going operations. Debates can begin (and can be won or lost) before military leaders have time to evaluate the issues and develop a response. Such debates can affect strategic goals, operational decision-making, tactical operations, morale and the overall effectiveness of the force involved. In effect, the GIE expands the AO to global proportions and is such an important source of information that it must be considered in all operational planning.

6. The Military Information Environment (MIE) consists of information systems and organizations, both friendly and adversary (or belonging to one of the belligerent factions in Operations Other Than War (OOTW)), military and non-military, that support, enable or significantly influence military operations. Information superiority is a key factor in the GIE and essential in the MIE if a commander is to achieve success. A commander must understand the pervasiveness and capability of the media, not only in their ability to report on an operation, but also on their ability to influence their target audiences with respect to the actual *legitimacy* of that operation.

7. A commander must anticipate how an adversary may attempt to use the media to achieve his own version of information superiority. The commander must also have the means to counter these attempts at misinformation and propaganda to mitigate the effects on the morale of his own troops. For example, during the Gulf war, Saddam Hussein targeted cities for Scud missile attacks that possessed international news media organizations. The intent was that media coverage of casualties and property damage would have a profoundly negative effect upon the targeted population, and produce a clear indication of Iraq's military

power. The coalition countered this attempt at media manipulation by, in turn, highlighting the capabilities of the Patriot missile batteries.

8. It can be argued that the presence of CNN in Baghdad also conformed to Saddam Hussein's plan for information superiority. With CNN reporting on the damage inflicted to that city by the coalition's so-called "smart" weapon systems, Saddam ensured that audiences around the world could see the pain and suffering of Iraqi civilians and call into question the effectiveness of the technology being employed against the Iraqi people. Perhaps more importantly, Hussein was able to escalate the anti-American fervour among his own people for his own warfighting purposes. These examples illustrate how commanders attempt to use or influence the media to achieve their goal of information superiority.

SECTION 3
ROLE OF PUBLIC AFFAIRS IN SUPPORT OF INFORMATION OPERATIONS

9. PA must be integrated with the other combat functions as it has a direct impact on the conduct of operations. Everything that the Army does to accomplish its mission occurs within the GIE. PA operations assist the commander in understanding and operating in the GIE by supporting his efforts to meet the information needs and expectations of internal and external audiences without compromising the mission.

10. The objective of PA is to help ensure information superiority by seizing the initiative with respect to media operations and putting in place programs which:

a. protect soldiers from the effects of enemy propaganda, misinformation and rumour; well-informed soldiers are effective soldiers;

b. support open, independent reporting and access to units and soldiers, (within the limitations of Operations Security (OPSEC));

c. establish the conditions leading to confidence in the Army; and

d. provide a balanced, fair and credible presentation of information that communicates the Army's story and

messages through an expedited flow of complete, accurate and timely information.

11. It must be noted that the role of PA is to *inform*, not to *influence*, which, by definition, is the role Psychological Operations (PSYOPS). Although it is possible that our target audiences may be influenced as a result of the information they receive, the key distinctions are the *intent* in providing the information and that PSYOPS must use governmental or military means for production and dissemination of their messages, not the media. PSYOPS can use information from the media to reinforce its messages, however PA must not be used to disseminate PSYOPS messages. Co-ordination is, however essential between PA and PSYOPS to ensure that there is no contradiction or divergence.

12. Commanders must understand that the *perception* of an operation can be as important to its success as the *execution* of that operation. PA must be considered and synchronized throughout the decision-making process **since everything that occurs in an operation has a PA dimension**. PA staffs support the commander by monitoring public perceptions and developing and disseminating clear and objective messages about military operations to external and internal audiences, thus ensuring operations are viewed in the proper context and can be understood.

13. Successful operations require an accurate assessment of the PA situation. The PA assessment is the continual analysis of the GIE and its potential impact on the operation. It provides the commander with a thorough examination of critical PA factors, such as:

a. the number, types and nationalities of news media representatives in the theatre;

b. the identification of any news media personalities and their parent organizations, as well as any reporting trends or biases;

c. news media needs and limitations;

d. news media communications and transportation capabilities; and

e. the perception of past, current or potential operations by internal and external audiences.

14. These must be taken into consideration when developing PA strategies and plans that support the commander's overall concept of operations.

15. The PA staff will develop a plan that not only supports the commander but also is in keeping with national level PA objectives. The potential impact of media coverage (and public reaction) on operations will be evaluated and the PA plan will address these potential impacts. However, in so doing, the fundamental PA principle regarding the expeditious flow of complete, accurate and timely information within the bounds of OPSEC will not be compromised.

16. PA strategies and plans are based on the following imperatives:

a. **Full integration of PA into the planning and decision-making process**. Fully integrated into the planning process at all levels, PA provides the commander with essential insights that must be weighed when visualizing the AO, assessing the situation and directing the military action required to achieve victory.

b. **Accurate assessment of the PA situation**. The PA assessment is the continual analysis of the information environment, both GIE and MIE, in order to assess its potential impact on the operation. It provides the commander with a thorough analysis of critical PA factors that must be considered in formulating and evaluating courses of action.

17. PA operations comprise four aspects:

a. **Planning**. PA planning is an integral part of the decision-making process and must be included at the very outset at all levels, from the strategic to the tactical. PAOs must be involved at every level in order to understand the higher commander's intent and to incorporate PA activities that effectively support his own commander's concept of operations and reflect national policy. PAOs seek to establish the conditions

which lead to confidence in the Army, and the operation, by ensuring an expedited flow of complete, accurate, and timely information that communicates the Army's perspective. This helps to ensure that media representatives understand the activities and events they are covering and report them in a balanced and fair way to our audiences, both external and internal. It also helps to reduce the constraints that inhibit the commander's range of possibilities and increases his freedom to act without distraction. Included in this planning aspect is the requirement to provide issues management and crisis communication advice to the commander and senior staff on a wide range of issues, operational and non-operational.

b. **Media operations**. Commanders, and their staffs, must accurately assess the level and intensity of media interest in their operation. For us to effectively communicate through the news media, we must anticipate their needs during all stages of an operation and do our best to accommodate them, without compromising OPSEC or the success of the mission. Media operations involve advising the commander on the implications of likely media reporting on his chosen course of action. Media operations also involve:

(1) Facilitating media coverage of operations, by anticipating and responding to the needs of the media. This is especially true of the media accompanying the troops on the ground. All media require accurate and timely information, as well as access to subject matter experts; however, in-theatre media representatives may have additional requirements such as transportation, accommodation and Communication Information System (CIS) support. Some media representatives may require rudimentary military survival training so as not to impose a danger to the troops they are covering, or themselves.

(2) Verifying media accreditation and assisting with accreditation, as required.

(3) Discussing the "ground rules" with respect to media coverage of on-going operations and ensuring enforcement, as required.

(4) Establishing and operating Public Affairs Operations Centres (PAOC).

c. **Internal Communication**. There is an essential requirement to inform our own troops throughout operations on issues that are related to operations, but also on other national (home) and international issues. This is an important morale and counter-PSYOPS activity that must be remembered when preparing and executing operations. These troop information activities are essential to the moral component of combat power. If a commander does not inform the troops someone else will with their own messages.

d. **PA training**. Given the level of media interest in all military operations, it is necessary that soldiers learn how to deal effectively with news media representatives, both on and off the battlefield. PA staffs have an important support role in this regard. Media awareness training must be provided to all deploying soldiers and, if practicable, should be extended to their families and rear party personnel as well.

SECTION 4
PUBLIC AFFAIRS PLANNING CONSIDERATIONS

18. The PA plan must be fully co-ordinated with the operational plan, usually becoming an annex to the operational plan. As a PA plan is developed, the following factors are considered:

a. **News media access**. To gain a complete understanding of the "big picture", journalists need access to deployed soldiers, units and formations. Media access must be planned and accommodated to the fullest extent possible. This will ensure that visiting news media do not compromise the mission nor endanger the soldiers that they are covering. Deployed forces must come to

expect media in their area, and they must be prepared to assist the news media in gaining access to areas accessible only by military means. Failure to plan for media access will result in unplanned media coverage. This may ultimately jeopardize the mission or otherwise have a detrimental effect on media (and the public's) understanding of the operation.

b. **Security**. OPSEC is a primary concern for mission planners and is a fundamental element in PA planning. The commander's security concerns must be addressed when planning where, and to what extent, news media will be allowed to visit and what can be said. Media access must be planned in advance and any restrictions must be consistently applied by the chain of command, in order not to compromise the chain of command and PA staff credibility. News media representatives are to be briefed at the earliest possible opportunity as to the guidelines with respect to reporting. Reporting guidelines will be promulgated as part of the overall operational plan. Nonconformity by media representatives may result in the suspension of visiting privileges. "Security at source" governs all conversations with the media and it must be emphasized that there is no such thing as an "off the record" interview.

c. **Media support**. Contingency planning should include provision for the equipment, transportation and communications assets necessary to help the accredited news media gather information and file stories about the operation. Arrangements with respect to using CIS assets, must be based on asset availability on a non-interference basis, and only in those cases where commercial services are unavailable.

d. **Internal information**. The needs of our internal audience must be considered in the PA planning process. Their understanding is critical and they rely on timely and accurate information from deployed units and formations. The news media is an important conduit for this information, but it cannot be relied upon to communicate our messages to our internal audience.

Other means of information passage, such as internal news organs, and the Internet, must be considered and form part of the PA plan for the operation.

SECTION 5
COMMAND AND CONTROL OF PUBLIC AFFAIRS

19. Deployed PA organizations must be mission capable, modular, flexible, agile, sufficiently equipped, and strategically positioned to support the commander in the battle for information superiority.

20. Once an operation begins, the priority of effort for the PA staff is to establish an identifiable PAOC to support the commander by sustaining the efforts of those news media representatives accompanying the units and to communicate with those news media representatives outside of the operation. In taking advantage of the principles of modularity and flexibility, the PAOC must expand its capability in concert with that of the deployed force. To be mission capable means that the PA staff must be able to respond to the commander's request for PA input into the operational plan, internal communication, as well as to meet the increasing demands of the news media covering the operation. Plans must be in place that will allow for the expansion of the PA organization, as required. This capability will help to ensure that a credible media relations infrastructure is in place, when needed, to reduce the chances of having uninformed and uncooperative news media representatives interfering with the operation. The PA organisation deployment must strike the delicate balance between between availability to conduct planning activities and manning of the PAOC. The PAOC must be where the media will be which is most often the last place where the commander wants to put his HQ.

21. The Army will often operate as part of a joint or multinational team. In joint operations where the major force is provided by the Army, the senior Army PAO will normally act as the lead PAO for the operation. It is understood that component HQs may have their own integral PA staffs; however, these PA staffs will focus primarily on internal communications activities. Contact with mews media representatives and organizations external to their component command will be co-ordinated through the PAOC of the lead component. In situations where other elements or agencies have the PA lead, the Army will provide PA personnel to help establish and operate a joint or multinational PAOC. On-going co-ordination and liaison between PA elements in a joint or

multinational PAOC is critical to ensure that the strategic goals of the operation, the Army's role in the operation, as well as security concerns and issues are clearly understood.

22. The PA function, is an essential and distinct support component of IO. The senior PAO is a specialist advisor to the commander and is responsible for the in-theatre co-ordination of media operations, PA planning, crisis communications and issues management (on-going media awareness training requirements will be co-ordinated through the general staff). The senior PAO also ensures that national policy and PA strategies are being incorporated into the commander's planning processes. In-theatre administrative support is mission dependent, but is provided by the supported headquarters.

23. As outlined in B-GL-300-003/FP-000, *Command,* a commander, to be effective requires a wide range of qualities and skills in addition to strictly military expertise. These include an understanding of national and international politics, world economics, foreign affairs, business management and planning, and the international laws of armed conflict. Different commanders will approach these challenges in different ways. The primary strength of the PAO will lie in the ability to assess how the commander wishes to address the PA challenges of command. The commander's PA concept of operations must be clearly understood by the PAO and in-theatre PA strategies and plans must take this imperative into consideration. Some commanders may wish to retain the role of official spokesperson for their formation; however, others may have a more decentralized approach, devolving authority to speak on substantive issues to subject matter experts. The PA staff supports the chain of command by ensuring that designated spokespersons are well prepared to speak with the media on these issues.

CHAPTER 8
CIVIL-MILITARY COOPERATION

The importance of the civilian dimension of the modern battlefield will not diminish; it will only loom larger. Senior leaders and commanders can no longer relegate Civil/Military Operations (CMO) planning to the status of an adjunct activity. CMO should be considered as important as the other combat functions.

Major T.E. Howie, US Army

SECTION 1
INTRODUCTION AND DEFINITIONS

1. Civil-Military Cooperation (CIMIC) has always been a component of military operations. CIMIC is an integral component of Information Operations (IO) as CIMIC provides vital information to the commander regarding the civil government and population, which will have an impact on his operations. CIMIC is defined as "*In peace, conflict and war, all measures undertaken between commanders and national authorities, civil, military and para-military, which concerns the relationship between the Canadian Forces, the national governments and civil populations in an area where Canadian military forces are deployed or plan to be deployed, supported, or employed. Such measures would also include cooperation and co-ordination of activities between commanders and non-governmental or international agencies, organizations and authorities.*"[15] CIMIC is the responsibility of commanders.

2. In the past, CIMIC focused on the military control of the civilian population in the Area of Operations (AO) to ensure that military operations were not hindered by civilians. This is particularly true during crisis and war. To illustrate this, Supreme Headquarters Allied Expeditionary Force (SHAEF) issued the following policy directive 1 May 1944: "A major responsibility of each commander is to ensure that conditions exist among the civilian population which will not interfere

---

[15] B-GG-005-004/AF-023, *Civil – Military Cooperation in Peace, Emergencies, Crisis and War*

with operations against the enemy, but will promote such operations to the greatest extent possible."[16]

3. As a stark contrast to warfighting, Operations Other Than War (OOTW) have changed how the Army views CIMIC. Entire military missions are now based on CIMIC in order to achieve the political objective. Providing humanitarian relief, assisting the United Nations High Commissioner for Refugees (UNHCR), and monitoring elections are but a few examples of how the military has been used to support civilians to achieve a political objective. CIMIC is conducted by military forces across the Spectrum of Conflict. In peace, the military will generally conduct operations that support the civilian population and governments. As the situation deteriorates/escalates the emphasis on CIMIC shifts from supporting civilian agencies to ensuring that military operations can continue at the warfighting end of the spectrum. This is illustrated in Figure 8-1-1.

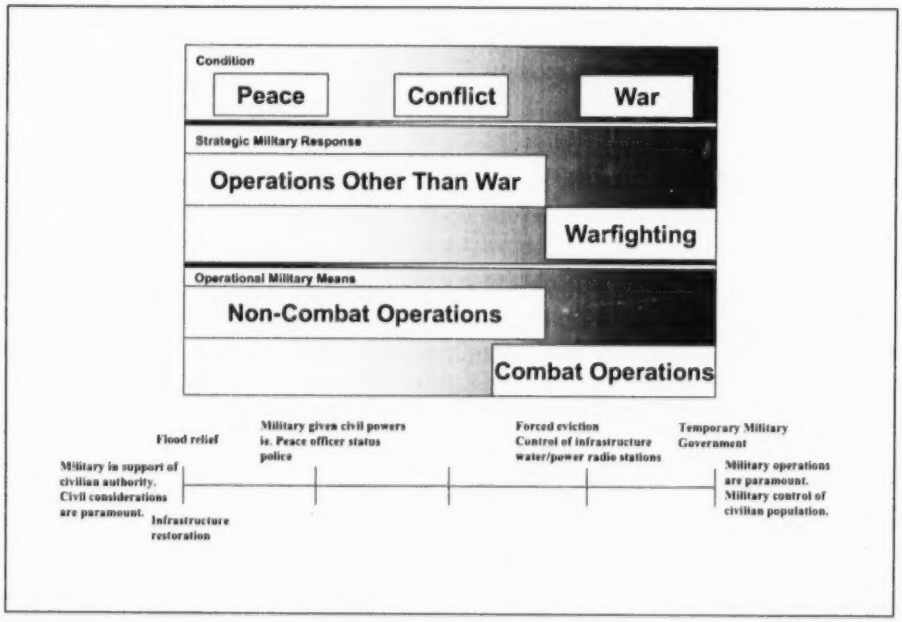

Figure 8-1-1: CIMIC and the Spectrum of Conflicts

4. Information gained through CIMIC is critical to the commander. Most military activities regarding civilians entail gaining information or

---

[16] Standard Policy and Procedures for Combined Civil Affairs Operations in North West Europe, 1 May 1944.

influencing their perceptions in order to gain cooperation (a last resort is the use of force). Even in wartime in a hostile territory, CIMIC activities will try to gain the support and cooperation of the civilian population so military operations are not jeopardised.

SECTION 2
ARMY OBJECTIVES IN CIVIL-MILITARY COOPERATION

5. The main objective of CIMIC is to achieve the necessary cooperation between civil authorities and the commander in order for the commander to achieve his aim. In domestic and international operations the Army's CIMIC objectives are basically the same as stated in the Canadian Forces manual:

a. support Canadian national interests;

b. fulfill obligations imposed by domestic law (National Defence Act, domestic laws) and international law (Law of Armed Conflict, International Human Rights Law) and such understanding and agreements reached between national authorities or parties;

c. advise, assist or reinforce foreign governments in accordance with national policy and operational requirements;

d. support the commanders mission;

e. support specific Canadian politico-military objectives in the theatre or AO;

f. assist the commander in support to civil administration;

g. facilitate the commanders mission by minimizing interference by the local population in the military phase of an operation and obtaining civil support for the civil phase and associated tasks;

h. assist the commander in meeting legal and moral obligations to the local population;

i. identify, and co-ordinate the use of local resources, facilities, and level of support for restoring local governments;

j. assist the commander, by providing those resources necessary to meet essential civil requirement, avoiding damage to civil property and usable resources, and minimizing loss of life and human suffering, assuming a dedicated CIMIC organization is available;

k. support as required International Organisations, Non-Governmental Organizations (NGOs), the UN and the Organization on Security and Cooperation in Europe (OSCE), as well as NATO or national civil agencies, in all types of civil-military cooperation, to a level specified by the Government or NDHQ; and

l. assist local authorities to create, restore and maintain public law and order.

6. The commander and staff must be very specific in their expectation of the functions to be performed under CIMIC. Figure 8-2-2 illustrates the scope and delineation of the type of operations the Land Forces can be expected to be involved in whether under the auspices of NATO or the UN.

Figure 8-2-2: The Operational Environment

SECTION 3
TYPES OF CIVIL-MILITARY COOPERATION

7. There are two types of CIMIC: civil-military operations and support to civil administration. Figure 8-3-3 illustrates the various components of CIMIC and their interrelationships to support a military operation.

8. Within the two types of CIMIC there are three functional areas:

a. **Negotiation of Co-ordination and Support Agreements**. These should be planned and negotiated by a single in-theatre authority as designated, during the early stages of campaign planning and cover all phases of the operation.

b. **Co-ordination of Civil-Military Support (CMS)**. CMS comprises all activities that entail civil-military interaction, co-ordination or cooperation.

c. **Co-ordination with Civil Emergency Planning (CEP)**. This is a national responsibility; there are considerations for both domestic and international environments which are explained in Canadian Forces Manual on CIMIC.

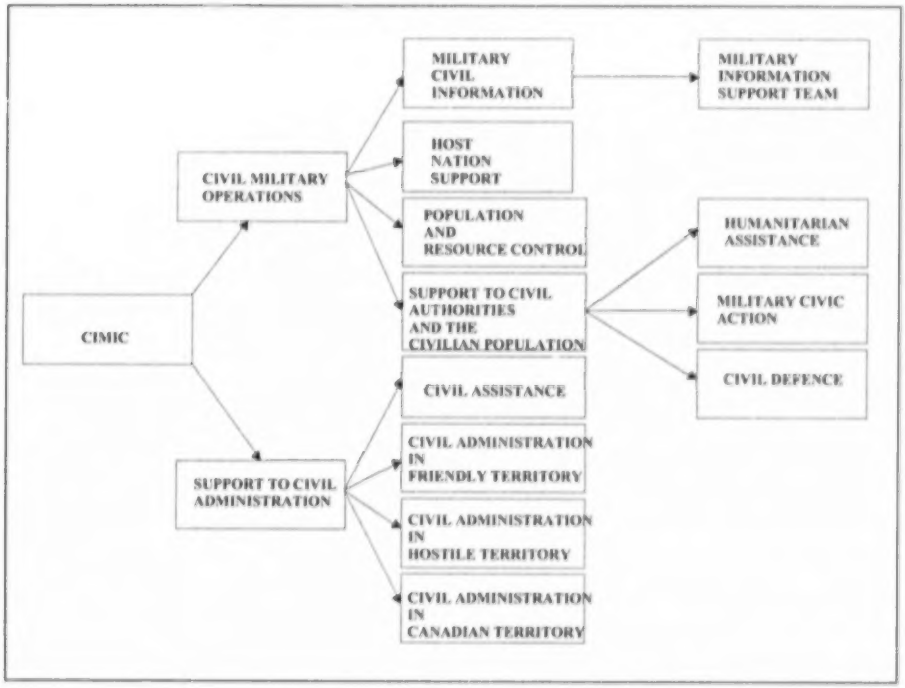

Figure 8-3-3: Types of Civil-Military Cooperation

SECTION 4
CIVIL-MILITARY COOPERATION, PSYCHOLOGICAL OPERATIONS AND PUBLIC AFFAIRS RELATIONSHIPS

9. The common ground between CIMIC, Psychological Operations (PSYOPS), and Public Affairs (PA) is information. CIMIC uses information to inform the in-theatre public on assistance programmes and reconstruction projects in their area. PA uses information to manage issues and inform the troops, Canadian as well as the public in the AO, of its activities in their area. PSYOPS uses information to attempt a change in perceptions, opinions, attitudes, behaviour, and beliefs of a population to gain support for civil tasks and of military and civilian activities. This will improve the unity of effort and bring about commitment of political and military leaders to create political, social, economic and

environmental conditions and change for a structural and sustainable peace.

10. CIMIC is an activity which the Canadian Forces and Army have conducted by other names, in domestic operations but principally in an "ad hoc" fashion in international operations. These "ad hoc" CIMIC activities were not however, integrated into the commanders plan.

SECTION 5
INFORMATION SOURCES

11. Information sources will vary depending of the area of CIMIC interest. Sources related to support of forces would mainly concern logistics, other nations, and local military leaders. Sources related to civilian environment would concern administrative structures, conditions of life, economy, humanitarian actions, and population. Main sources are as follows:

a. **Interpreters**. Local interpreters are one of the best sources of local information. Caution is required in that they may attempt to pursue a personal or factional agenda. They have an intimate knowledge of the local politics, society and customs. They will immediately know who is to be addressed, and be able to perceive abnormal situations. They are recognized by local population as one of them, and are answered more spontaneously than any CIMIC personnel. Interpreters are a vital part of the CIMIC team. Their value is much more than their abilities to speak the local language. However, a duality of purpose exists in the context of interpreters being part of the CIMIC team. They spontaneously try to satisfy the requirements of their position while holding onto their personal beliefs and ideals. They must be used with sagacity and their loyalty must be checked periodically. Local interpreters should be supplemented by military interpreter in cases where the issue is sensitive or critical to the success of the mission.

b. **Organizations and Agencies.** National and International Agencies, foreign governments, Private Voluntary Organizations (PVOs), NGOs, various

organizations are excellent sources of CIMIC information and support. These organizations have usually been in country much longer than our force and have a valuable "outsiders" perspective of local activities that is worthy of interpretation. CIMIC personnel contact with these entities is in an informal manner without any of the military formalities. The amount of interaction or protection and therefore contact with an individual organization is a function of the organization's charter. Some are more open to military assistance then others.

c. **Refugees**. In general, refugees psychological fragility leads them to be very expressive of personal events and occurrences on their journey, however, their interpretation of events is often distorted by their shock or trauma. Any information obtained from refugees should be passed to intelligence staff for processing.

d. **Political, Religious or Ethnical Factions**. The leadership of factions are the usual point of contact for CIMIC personnel. It is necessary to make contact with each to maintain an objective impartiality. There is however a tendency among special interest groups to explain their "Particular" position and therefore it may be difficult to establish the truth. Nonetheless, it is desirable to establish contact or have knowledge of these factions. But, again, any information obtained from these factions should be passed to intelligence staff as a matter of course.

e. **Population**. Inside the local population, there is a value in speaking to the ordinary person. It is a way to gauge the local climate and information gained at higher levels. A grassroots understanding of current lifestyles, preoccupations and local concerns, is a first step in the analysis of both your information sources and the results of your CIMIC actions. This in turn allows the Ops Cell to anticipate on possible events resulting from the evolution of the current situation.

SECTION 6
CIMIC AND INFORMATION PROCESSING

12. The primary mission of CIMIC is to support operations. Their ability to transmit and gather information must be balanced with the need to accomplish the primary mission. Outgoing and incoming CIMIC information must follow a recognized path through the forces and integrate with the normal planning process.

a. **Identification of the Requirement**. Even if gathering information is an elementary reflex for CIMIC personnel, particular needs have to be initiated through Battle Procedure. The Civil-Military Operation Centre (CMOC) acts as the primary focal point for CIMIC information gathering.

b. **Planning**. The CMOC is responsible for drafting the CIMIC collection plan. It includes the G5 directives, the commander's intent and orientations, input from intelligence and G3 branch. Information objectives may not be readily obtainable because the CIMIC mission is the primary goal. The Commander's Critical Information Requirements (CCIR) must be used to provide direction on CIMIC involvement in information gathering.

c. **Gathering Information**. CMOC assigns the requests for info with the attached Canadian constraints, and waits for the returns. CIMIC personnel report back to the CMOC Ops O. This officer screens and correlates the reports, and forewords them to the Intelligence Cell. They also return a report concerning the request for info to the concerned branches. As expressed earlier, the CMOC Ops O must be aware of possible misinformation actions against the Canadian Forces and must be vigilant.

d. **Interactions**. CIMIC staff must remember that they are an information asset in support of operations. A constant liaison is to be established with the Ops Cell, and a technical link with the Intelligence Cell and the PAO. At the same time, other branches must be

checked periodically to make sure that communications are being passed.

e. **Periodic CIMIC assessment**. A CIMIC assessment update must be issued periodically to the general staff indicating the current situation. In case of significant changes in CIMIC assessment, G5 must report to the Chief of Staff and make a new proposal. In Information Operations, G5 is no more than an asset in support of operations.

SECTION 7
LIMITATIONS/UNAUTHORIZED ACTIVITIES

13. CIMIC, PSYOPS, and PA functions must be carefully co-ordinated and managed so as not to overstep the scope of their activities, otherwise they may compromise themselves. In essence, neither one of the organizations should conduct a campaign that would impair each other's operations. Therefore, co-ordination and synchronization of activities between these organizations is paramount to the attainment of the commander's mission.

14. In most cases, CIMIC personnel can get the freedom of movement necessary to fulfil their mission. However, there may be periods where the level of hostilities prevents CIMIC personnel from being as active as they need to be. Personnel may face high risks and be given little protection while trying to accomplish their mission. At these times the staff may need to revise the CIMIC plan or some of its internal priorities.

ANNEX A
MUTUAL SUPPORT WITHIN THE ELEMENTS OF OFFENSIVE AND DEFENSIVE INFORMATION OPERATIONS

	OPSEC	CI	MILITARY DECEPTION	PSYOPS	COUNTER-PSYOPS	EW	CNA	SPECIAL IO	PHYSICAL DESTRUCTION
OPSEC		CI estimate determines OPSEC parameters and threats CI activities support OPSEC	Concealing competing observables Degrading general situation information to enhance effect of observables	Concealing competing information Degrading general situation to enhance effect of PSYOPS	Determines adversary PSYOPS threat to be countered	Concealing EW units and systems to deny information on the extent of ESM/ECM capabilities	Conceals friendly CNA capabilities	As determined by the nature of the SIO. Any or all elements may be used to support SIO	Concealing dedicated systems for Off IO to deny information on the extent of Off IO capabilities
CI	OPSEC measures compensate for vulnerabilities identifies by CI		Assist in determining the adversary susceptibility to deception	Conceal our PSYOPS capability	N/A	Confirms CI successes	Provides feedback on success of CNA	As determined by the nature of the SIO. Any or all elements may be used to support SIO	Provides form of BDA
MILITARY DECEPTION	Influencing adversary not to collect against protected units activities Influencing adversary to underestimate friendly OPSEC Providing information to fill 'gaps' created by friendly OPSEC	Confuse adversary ISTAR capabilities		Providing information compatible with PSYOPS theme Reinforcing PSYOPS theme in content of deception	Makes adversary believe that PSYOPS will not be effective	Influencing adversary to: Underestimate friendly ESM/ECM capabilities Defend wrong C2 systems from friendly ESM/ECM	Makes adversary more prone to the affects of CNA	As determined by the nature of the SIO. Any or all elements may be used to support SIO	Influencing adversary to: Underestimate friendly Off IO destruction capabilities Defend wrong C2 element/system from friendly ISTAR destruction
PSYOPS	Protecting information on OOTW Creating perception that fits OPSEC activities	Assist in identifying targets for PSYOPS	Creating perceptions and attitudes that can be exploited by military deception Integrating PSYOPS actions with deception		Helps set conditions for effective PSYOPS	Broadcasting PSYOPS assets to disseminate products on adversary frequencies Developing messages for broadcast on other service EW assets	Makes adversary believe our CNA capabilities are much more effective than in reality	As determined by the nature of the SIO. Any or all elements may be used to support SIO	Causing populace to flee target areas Reducing collateral damage limitations on destruction of adversary C2 infrastructure

	OPSEC	CI	MILITARY DECEPTION	PSYOPS	COUNTER -PSYOPS	EW	CNA	SPECIAL IO	PHYSICAL DESTRUCTION
COUNTER-PSYOPS	Improves OPSEC posture	Identifies and neutralizes agents of influence (both friendly and adversary)	Identifies an adversary use of PSYOPS as a deception	Counter effect of adversary use of PSYOPS		Assist in determining the success of ECM	Reduces adversary use of PSYOPS through CNA	As determined by the nature of the SIO. Any or all elements may be used to support SIO	Reduces adversary PSYOPS effects on units
EW	Degrading adversary ISTAR in EM spectrum against protected units and activities Covering "short term" gaps in OPSEC	Assist in determining the adversary's capability to conduct ESM/ECM	Conducting ESM/ECM deception Degrading adversary capability to see, report and process competing observables Isolating decision makers from information at critical times to enhance effects of deception executions	Degrading adversary capability to see, report and process conflicting information Isolating target audience from conflicting information	Assist in determining success of the COUNTER-PSYOPS program		Used as a means to conduct CNA	As determined by the nature of the SIO. Any or all elements may be used to support SIO	Provide Off IO target acquisition through ESM Destroying or upsetting susceptible assets using EMS with ECM
CNA	Convince adversary that OPSEC posture is better than it is	Attack adversary ISTAR capabilities	CNA used a component of deception	Reduces an adversary's confidence in his own computer networks	Attack means used by adversary PSYOPS	N/A		As determined by the nature of the SIO. Any or all elements may be used to support SIO	Used in conjunction with other destruction.
SPECIAL IO	Assist or support other elements as necessary	Assist or support other elements as necessary	Assist or support other elements as necessary	Assist or support other elements as necessary	Assist or support other elements as necessary	Assist or support other elements as necessary	Assist or support other elements as necessary		Assist or support other elements as necessary
PHYSICAL DESTRUCTION	Preventing or degrading adversary ISTAR against protected units and activities	Identify an neutralize saboteurs	Conducting attacks as deceptions Degrade adversary capabilities to see, report and process competing observables Isolating decision maker from information at critical times to enhance effect of deception	Degrading adversary capability to see, report and process conflicting information Degrading adversary capability to jam PSYOPS broadcast Isolating target audience from conflicting information	Degrade an adversary PSYOPS capability	Reducing friendly ECM target set for Def IO by selective and co-ordinated destruction of adversary C2 Destroying selected electronic systems to force adversary use of systems susceptible to friendly ESM/ECM	Degrade an adversary's ability to conduct CNA	As determined by the nature of the SIO. Any or all elements may be used to support SIO	